S. HRG. 106-527

CYBERCRIME: CAN A SMALL BUSINESS PROTECT ITSELF?

FORUM

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MARCH 9, 2000

Printed for the Committee on Small Business

U.S. GOVERNMENT PRINTING OFFICE
64-617 cc WASHINGTON : 2000

COMMITTEE ON SMALL BUSINESS

ONE HUNDRED SIXTH CONGRESS

CHRISTOPHER S. BOND, Missouri, *Chairman*

CONRAD BURNS, Montana
PAUL COVERDELL, Georgia
ROBERT F. BENNETT, Utah
OLYMPIA J. SNOWE, Maine
MICHAEL ENZI, Wyoming
PETER G. FITZGERALD, Illinois
MIKE CRAPO, Idaho
GEORGE V. VOINOVICH, Ohio
SPENCER ABRAHAM, Michigan

JOHN F. KERRY, Massachusetts
CARL LEVIN, Michigan
TOM HARKIN, Iowa
JOSEPH I. LIEBERMAN, Connecticut
PAUL D. WELLSTONE, Minnesota
MAX CLELAND, Georgia
MARY LANDRIEU, Louisiana
JOHN EDWARDS, North Carolina

EMILIA DISANTO, *Staff Director*
PAUL COOKSEY, *Chief Counsel*
PATRICIA R. FORBES, *Democratic Staff Director and Chief Counsel*

CONTENTS

Page

PARTICIPANTS

COMMENT FOR THE RECORD

*Comments (if any) between pages 56 and 88.

CYBERCRIME: CAN A SMALL BUSINESS PROTECT ITSELF?

THURSDAY, MARCH 9, 2000

UNITED STATES SENATE,
COMMITTEE ON SMALL BUSINESS,
Washington, D.C.

The Committee met, pursuant to notice, at 9:41 a.m., in Room SR–428A, Russell Senate Office Building, The Honorable Christopher S. Bond (Chairman of the Committee) presiding.

Present: Senators Bond, Burns, and Kerry.

OPENING STATEMENT OF THE HONORABLE CHRISTOPHER S. BOND, CHAIRMAN, SENATE COMMITTEE ON SMALL BUSINESS, AND A UNITED STATES SENATOR FROM MISSOURI

Chairman BOND. Good morning. The Committee on Small Business welcomes you to its second forum of the 106th Congress. This forum is entitled "CyberCrime: Can a Small Business Protect Itself?"

I have to apologize for the delay in starting. We have had so much interest on this, I stopped to do some media interviews on the way in because people are finally beginning to realize how important this subject is. Senator Burns tells me that in the Commerce Committee he has just held a hearing on this. We want to focus particularly on small businesses and the vulnerability of small businesses, and what we can do about it.

We have some real experts here today, some people who have had experience with this issue. I remember from unsuccessful political ventures of mine, friends after a significant loss have slapped me on the back and told me that experience is what you get when you expect to get something else. We believe we can learn from some of the experiences we will be told about today.

Nine months ago this Committee held a forum on e-Commerce and its potential to allow a small business to compete successfully against its giant competitors. At that forum we outlined some of the obstacles to success in this dynamic market. The goal of this forum is to raise awareness of CyberCrime and to generate a dialogue between law enforcement and the small business community.

According to a study by the University of Texas, e-Commerce accounted for the creation of 1.2 million jobs and $300 billion in revenue in 1998 alone. We all recognize what an astonishing growth pattern that is and the pace of it is truly remarkable. What is even more impressive is a recent Forrester Research study concluded that in January 2000 alone there was $2.8 billion in online retail

sales, greater than the total $2.4 billion of retail sales for the entire year of 1997.

We expect growth in this area to continue with increasingly more business being conducted via the Internet, both through e-retail and through more conventional business-to-business e-Commerce. With such expanded business activity, however, come new threats that we must address. A prime example is computer crime.

The extent of the threat is truly alarming. The most accurate data that we have available comes to us from the Computer Emergency Response Team, or CERT as its known, at Carnegie Mellon University. We plotted that data on the chart to my right. What we see is a 121 percent increase in intrusion incidents like "hacking" reported from 1998 to 1999. For some of you it is a little hard to see with the lights, but you see a slowly rising curve to 1997 and it goes up sharply in 1998 and almost straight up in 1999. Recent research by the Computer Security Institute indicates that 30 percent of businesses nationwide have been victimized by computer intrusions.

It is important to note that many companies have been the victim of hacker attacks, yet fearing negative publicity and reduced consumer confidence, they have been reluctant in too many instances to report such incidents. Over time many of the Nation's largest businesses have been actively working to protect themselves from computer criminals and computer vandals whose actions can cause considerable harm. I am concerned that with greater efforts on the part of Government, and as big business does take steps to protect itself, small business will become a much more inviting target.

This is even more timely given the recent case where a home-based business in Oregon was reported to have its computer hacked and used in the so-called "denial of service" attacks on the web sites of Yahoo, eBay, CNN, Amazon.com and others. These recent attacks should serve as a useful wake-up call to business, Government and academia. Nearly 2 years ago, CERT warned the industry of the potential of a such an attack. These warnings were repeated by the National Infrastructure Protection Center at the FBI. Unfortunately, it appears that the warnings have not had their necessary impact.

We have today a panel of experts, Joan Neptune from LC Communications in Florida was a victim of computer crime and she will share her personal experience; Special Agent Mary Riley from the Secret Service, the head of the Electronic Crimes Branch; Scott Charney from PricewaterhouseCoopers, formerly chief of the computer crime section at the Department of Justice; and we will hear from Roger Farnsworth, manager of product marketing at Cisco Systems. Cisco is the world's largest manufacturer of equipment that connects people and businesses.

But before turning to our panelists, let me encourage everyone here today to take an active part in the discussion portion. I hope that everyone will think about areas where this Committee can be of assistance, either encouraging dialogue, by providing a voice for small businesses, or if there are legislative fixes needed.

We will be producing a formal transcript of the forum and we will hold the record open for 2 weeks to invite additional state-

ments that any of you would like to submit. I would extend that to our audience both here and the people who are watching us via live transmission on the Committee's web site.

Before turning to the panelists, obviously it is always a pleasure to turn to my partner in this operation, the distinguished Senator from Massachusetts, Senator Kerry.

Welcome, Senator Kerry.

[Attachments to the statement of Senator Bond follow:]

CERT/CC Statistics 1988-1999

CERT/CC Statistics 1988-1999

The CERT/CC publishes statistics for:

- Number of incidents reported
- Vulnerabilities reported
- Security alerts published
- Security notes published
- Mail messages handled
- Hotline calls recieved

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1991	1993	1995	1997	1999
Incidents	406	1,334	2,412	2,134	8,268

Total incidents reported (1988-1999): **24,364**

Vulnerabilities reported

1995-1999

Year	1996	1998	1999
Vulnerabilities	345	262	9

Total vulnerabilities reported (1995-1999): **1,508**

Security alerts published

1988-1989

Year	1989
Advisories	7
Vendor Bulletins	
Summaries	
Totals	7

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Advisories	12	23	21	19	15	18	24	28	13	17
Vendor Bulletins					2	10	2	16	3	
Summaries						3		6		5
Totals	12	23		19	17	31		50	4	22

Total security alerts published (1988-1999): **290**

Security notes published

1998-1999

Year	1998	1999
Incident notes		8
Vulnerability notes	18	3
Total notes	15	11

Total security notes published (1998-1999): **26**

Mail messages handled

1988-1989

Year	1989
Mail	2,869

1990-1999

Year	1991	1993	1995	1997	1999
Mail	9,629	21,267	32,084	39,626	32,967

Total mail messages handled (1988-1999): **260,610**

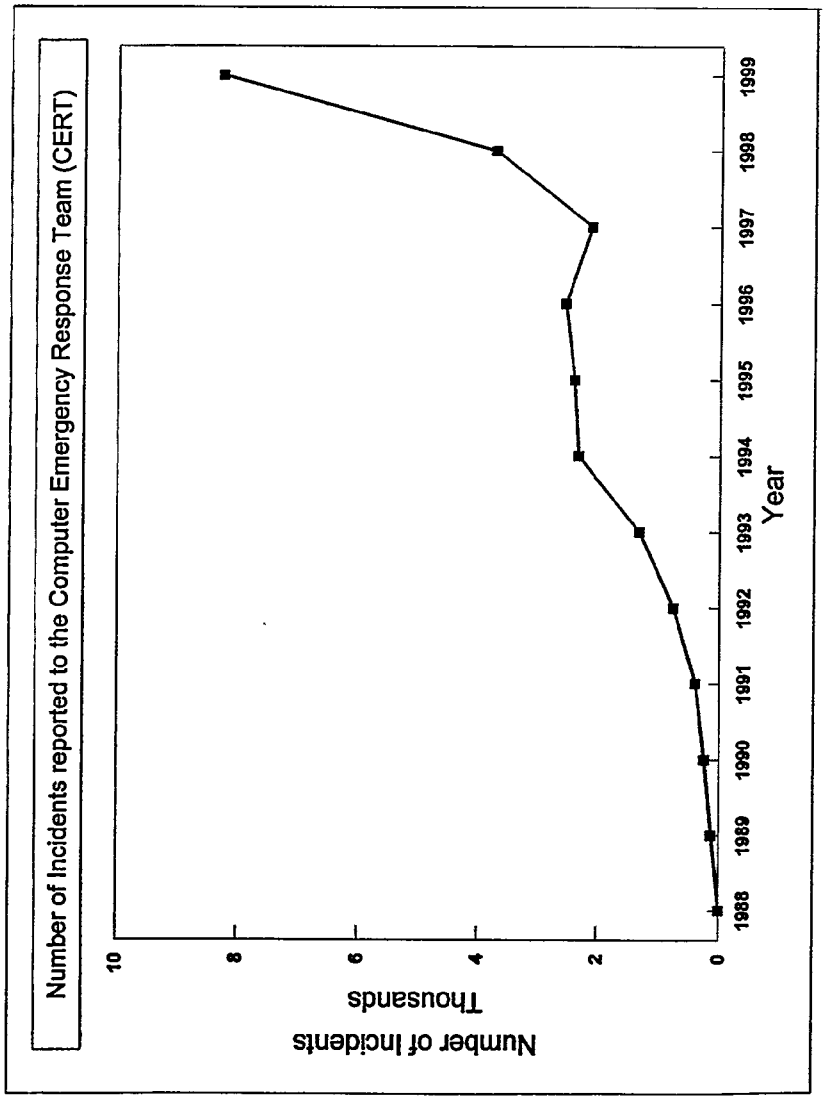
Hotline calls received

1992-1999

Year	1993	1995	1997	1999
Calls	2,282	3,428	1,058	2,099

Total hotline calls received (1992-1999): **17,626**

This page was last updated on January 20, 2000.



CSI Press Release - March 5, 1999

March 5, 1999
FOR IMMEDIATE RELEASE
Contact: Patrice Rapalus, Director
Computer Security Institute
600 Harrison Street
San Francisco, CA 94107
415/905-2310

2000 Survey Coming Soon!

For a free paper copy upon publication April 2000, "Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey," complete with graphs, charts and analysis, please fill out the Survey Request Form

Internet: prapalus@mfi.com

Cyber attacks rise from outside and inside corporations

Dramatic increase in reports to law enforcement

SAN FRANCISCO -- The Computer Security Institute (CSI) announced today the results of its fourth annual "Computer Crime and Security Survey." The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation (FBI) Computer Intrusion Squad. The aim of this effort is to help raise the level of security awareness as well as determine the scope of computer crime in the United States.

Highlights of the "1999 Computer Crime and Security Survey" include the following: Corporations, financial institutions and government agencies face threats from outside as well as inside.

System penetration by outsiders increased for the third year in a row; 30% of respondents report intrusions.

Those reporting their Internet connection as a frequent point of attack rose for the third straight year; from 37% of respondents in 1996 to 57% in 1999.

Meanwhile, unauthorized access by insiders also rose for the third straight year; 55% of respondents reported incidents.

Other types of cyber attack also rose. For example, 26% of respondents reported theft of proprietary information.

Perhaps the most striking result of the 1999 CSI/FBI survey is the dramatic increase in the number of respondents reporting serious incidents to law enforcement: 32% of respondents did so, a significant increase over the three prior years, in which only 17% had reported such events to the authorities.

For the third straight year, financial losses due to computer security breaches mounted to over a $100,000,000. Although 51% of respondents acknowledge suffering financial losses from such security breaches, only 31% were able to quantify their losses. The total financial losses for the 163 organizations that could put a dollar figure on them add up to $123,779,000.

The most serious financial losses occurred through theft of proprietary information (23 respondents reported a total of $42,496,000) and financial fraud (27 respondents reported a total of $39,706,000).

Summary data for responses to all 1999 survey questions and a table displaying financial losses due to various types of security breachrs reported in 1997, 1998 and 1999 accompany this press release.

Although these survey results indicate a wide range of computer security breaches, perhaps the most disturbing trend is the continued increase in attacks from outside the organization. This trend was reinforced by other survey results. For example, of those who acknowledged unauthorized use, 43% reported from one to five incidents originating outside the organization, and 37% reported from one to five incidents originating inside the organization.

Further evidence of increased system penetration from the outside can be gleaned from a series of questions on WWW sites and electronic commerce that were asked for the first time this year. Ninety-six percent of respondents have WWW sites, 30% provide electronic commerce services. Twenty percent had detected unauthorized access or misuse of their WWW sites within the last 12 months (disturbingly, 33% answered "don't know.")

Of those who reported unauthorized access or misuse, 38% reported from two to five incidents, and 26% reported 10 or more incidents Thirty-eight percent reported that the unauthorized access or misuse came from outside. Several types of attack were specified. 98% reported vandalism, 93% reported denial of service, 27% reported financial fraud, 25% reported theft of transaction information. Only 12 of the 95 respondents who had their WWW sites attacked could quantify their financial losses The total losses for the 12 respondents totaled $2,383,000 (an average of $198,583 in financial losses for each respondent.)

Based on responses from 521 security practitioners in U.S. corporations, government agencies, financial institutions and universities, the findings of the "1999 Computer Crime and Security Survey" confirm trends established over the last three annual surveys. It is clear that computer crime and other information security breaches pose a growing threat to U.S. economic competitiveness and the rule of law in cyberspace. It is also clear that the financial cost is tangible and alarming.

Sixty-two percent of respondents reported computer security breaches within the last twelve months.

The breaches detected by respondents include a diverse array of serious attacks, several of which rose in the number of reports from 1998 to 1999; for example, system penetration by outsiders, unauthorized access by insiders and theft of proprietary information as mentioned above.

Here are some other examples.

Denial of service attacks were reported by 32%.

Sabotage of data or networks was reported by 19%.

Financial fraud was reported by 14%.

Insider abuse of Internet access privileges (for example, downloading pornography or pirated software or engaging in inappropriate use of e-mail systems) was reported by 97%.

This increase indicates that the danger of entanglement in civil liability suits is also on the rise.

Virus contamination was reported by 90%.

Laptop theft was reported by 69%.

Patrice Rapalus, CSI director, suggests that organizations pay more attention to information security staffing and training. "It is interesting to note that while many respondents answered 'yes' to the use of sophisticated security technologies, serious breaches continue to increase. It is also significant that so many respondents answered 'don't know' to whether or not their WWW sites had been attacked. Corporations and government agencies that want to survive in the 'Information Age' simply have to dedicate more resources to staffing and training of information security professionals. Furthermore, information security professionals who want to succeed have to increase their own level of technical acumen in order to face the challenges ahead."

Michael A Vatis, Director of the National Infrastructure Protection Center, FBI headquarters, Washington, D.C., observed that "this year's CSI/FBI study confirms the need for industry and government to work together to address the growing problem of computer intrusions and cyber crime generally. Only by sharing information about incidents, and threats, and exploited vulnerabilities can we begin to stem the rising tide of illegal activity on networks and protect our nation's critical infrastructure from destructive cyber attacks."

###

CSI, established in 1974, is a San Francisco-based association of information security professionals. It has thousands of members worldwide and provides a wide variety of information and education programs to assist practitioners in protecting the information assets of corporations and governmental organizations.

The FBI, in response to an expanding number of instances in which criminals have targeted major components of

information and economic infrastructure systems, has established National Infrastructure Protection and Computer Intrusion Squads in selected offices throughout the United States. The mission of these squads is to investigate violations of Computer Fraud and Abuse Act of 1986, including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes where the computer is a major factor in committing the criminal offense.

The seriousness of this mission was recently reinforced by the creation of the National Infrastructure Protection Center, located at FBI headquarters. Recognizing this country's unprecedented reliance on information technology, the Center, which is a joint partnership among federal agencies and private industry, is designed to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nation's infrastructures. (These infrastructures include telecommunications, energy, transportation, banking and finance, emergency services and government operations).

CSI Press Release - March 5, 1999

For a free paper copy of the final report, "Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey," complete with graphs, charts and analysis, please e-mail your postal address to prapalus@mfi.com

1999 CSI-FBI Survey Results

#1 What category describes your organization's activity?

		%of answered (521)
Utility	22	4%
Manufacturing	63	12%
Financial	104	20%
Telecommunications	28	5%
Transportation	7	1%
High-tech	63	12%
Medical	35	7%
Retail	12	2%
Education	26	5%
Federal Gov.	40	8%
State Gov.	23	4%
Local Gov.	7	1%
Other	91	17%
Totals	521	100%

#2 What is the number of employees in your organization?

	1 to 99	61	12%
TOTALS	100 to 499	61	12%
	500 to 999	36	7%
	1000 to 5000	139	27%
	5001 to 9999	55	11%
	10000 or more	164	31%
	Answered question	516	99%
	Total possible:	521	

#3 If your organization is a commercial enterprise, what is its gross income?		%of total (521)	%of answered (357)
Under $10 million	59	11%	17%

$11-99 million	55	11%	15%
$100-500 million	56	11%	16%
$501 million - 1 billion	36	7%	10%
Over 1 billion	151	29%	42%
Answered question	357	69%	100%

#4 What following types of security technology do you use?		%of total (521)	% of answered (501)
access control	465	89%	93%
biometrics	43	8%	9%
encrypted files	305	59%	61%
anti-birus software	490	94%	98%
reusable passwords	305	59%	61%
firewalls	456	88%	91%
encrypted log-in/sessions	229	44%	46%
physical security	458	88%	91%
PCMCIA, smart cords, one-time tokens	193	37%	39%
intrusion detection	211	40%	42%
digital Ids, certificates	168	32%	34%
Answered question	501	96%	100%

#5 Has your organization experienced unauthorized use of computer systems in the last year?		%of total (521)	% of answered (512)
Yes	319	61%	62%
No	87	17%	17%
I don't know	106	20%	21%
Answered question	512	98%	100%

#6 If yes, how many incidents?		%of total (521)	% of answered (327)
1 to 5	112	21%	34%
6 to 10	73	14%	22%
11 to 30	24	5%	7%
31 to 60	7	1%	2%
Over 60	15	3%	5%
Don't know	96	18%	29%
Answered question	327	63%	100%

#7 How many of these were from outside the organziation?	%of total (521)	% of answered (280)

1 to 5	121	23%	43%
6 to 10	23	4%	8%
11 to 30	14	3%	5%
31 to 60	3	1%	1%
Over 60	9	2%	3%
Don't know	110	21%	39%
Answered question	280	54%	100%

#8 How many of these were from inside the organziation?		%of total (521)	% of answered (308)
1 to 5	113	22%	37%
6 to 10	49	9%	16%
11 to 30	28	5%	9%
31 to 60	2	0%	1%
Over 60	7	1%	2%
Don't know	109	21%	35%
Answered question	308	59%	100%

#9 On a scale from 1 - 4, indicate the rate of frequency with which the following systmes have been attacked.

	Less frequent	More frequent	total
Internal systems	159	164	323
	49%	51%	62%
Remote dial-in	216	84	300
	72%	28%	58%
Internet access	140	184	324
	43%	57%	62%

>#10. Indicate each of the following as likely sources of attack.

	Unlikely	Likely	Totals
Foreign gov.	332	90	422
	79%	21%	81%
Foreign corp.	297	130	427
	70%	30%	82%
Independent Hackers	117	336	453
	26%	74%	87%
US competitor	201	227	428
	47%	53%	82%
Disgruntled employee	64	396	460
	14%	86%	88%

#11. Which of the following types of electronic attack or misuse has your organiziation detected in the last year?		%of total (521)	% of answered (405)
Theft of proprietary info	104	20%	26%
Sabotage of data or networks	78	15%	19%
Telecom eavesdropping	53	10%	13%
System penetration by outsider	124	24%	31%
Insider abuse of net access	394	76%	97%
Financial fraud	58	11%	14%
Denial of service	128	25%	32%
Virus contamination	365	70%	90%
Unauthorized access to info by insider	223	43%	55%
Telecom fraud	70	13%	17%
Active wiretapping	9	2%	2%
Laptop theft	280	54%	69%
Answered question	405	78%	100%

#12 Which of the following types of electronic attack or misuse has caused your organization financial loss?		%of total (521)	% of answered (265)
Theft of proprietary info	61	12%	23%
Sabotage of data or networks	49	9%	18%
Telecom eavesdropping	12	2%	5%
System penetration by outsider	52	10%	20%
Inseder abuse of net access	182	35%	69%
Financial fraud	53	10%	20%
Denial of service	74	14%	28%
Virus contamination	231	44%	87%
Unauthorized access to info by insider	85	16%	32%
Telecom fraud	48	9%	18%
Active wiretapping	2	0%	1%
Laptop theft	249	48%	94%
Answered question	265	51%	100%

#13 Indicate the approximate $ value that you've lost.		
Theft of proprietary info	$42,496,000	34%
Sabotage of data or networks	$4,421,000	4%
Telecom eavesdropping	$765,000	1%
System penetration by outsider	2,888,000	2%

Insider abuse of net access	$7,576,000	6%
Financial fraud	$39,706,000	32%
Denial of service	3,255,000	3%
Virus contamination	$5,274,000	4%
Unauthorized access to info by insider	$3,567,000	3%
Telecom fraud	$773,000	1%
Active wiretapping	$20,000	0%
Laptop theft	$13,038,000	11%
TOTALS:	$123,779,000	100%

#13 CONTNUED	Number answered	% of answered (163)
Theft of proprietary info	23	14%
Sabotage of data or networks	27	17%
Telecom eavesdropping	10	6%
System penetration by outsider	28	17%
Inseder abuse of net access	81	50%
Financial fraud	27	17%
Denial of service	28	17%
Virus contamination	116	71%
Unauthorized access to info by insider	25	15%
Telecom fraud	29	18%
Active wiretapping	1	1%
Laptop theft	150	92%
TOTAL Answered	163	100%

#14 Does your organization have a WWW site?			% of answered (513)
Yes	490	94%	96%
No	23	4%	4%
Answered question	513	98%	100%

#15 Does your organization provide electronic commerce services via WWW site?			% of answered (510)
Yes	151	29%	30%
No	358	69%	70%
Answered question	510	98%	100%

#16. If yes, what are the annual revenues from these services?		
Total	$617,176,000	
Answered question	36	7%

#17 Has your WWW site suffered unauthorized access or misuse within the last 12 months?		%of total (521)	% of answered (479)
Yes	95	18%	20%
No	227	44%	47%
Don't know	156	30%	33%
Answered question	479	92%	100%

#18. If yes, how many incidents?		%of total (521)	% of answered (92)
one	28	5%	30%
2 to 5	35	7%	38%
5 to 9	3	1%	3%
10 or more	26	5%	28%
Answered question	92	18%	100%

#19. If yes, did the attacks come from insiders or outsiders?		%of total (521)	% of answered (159)
Inside	9	2%	7%
Outside	47	9%	38%
Both	51	10%	41%
Don't know	18	3%	14%
Answered question	125	24%	100%

#20 If yes, please specify the type of unauthorized access or misuse.		%of total (521)	% of answered (44)
Vandalism	43	8%	98%
Financial fraud	12	2%	27%
Denial of service	41	8%	93%
Theft of transaction info	11	2%	25%
TOTAL	44	8%	100%

#21 If yes, what financial losses did your organization suffer due to the incident?		
Total	$2,383,000	
Answered question	12	2%

#22 Would your organzation consider hiring as consultants reformed hackers?		%of total (521)	% of answered (506)
Yes	85	16%	17%
No	327	63%	65%

Don't know	94	18%	19%
Answered question	506	97%	100%

#23 If your organzation has expericned computer intrusions within the last 12 months, what did you do?		%of total (521)	
Did your best to patch security holes	283	54%	96%
Did not report intrusions	142	27%	48%
Reported intrusions to law enforcement	95	18%	32%
Reported intrusions to legal counsel	87	17%	29%
Answered question	295	57%	100%

#24 If your organzation didn't report the intrusions, list the reasons:

	Less important	More important	TOTALS
Negative publicity	23	84	107
	21%	79%	21%
Competitiors	32	60	92
	35%	65%	18%
Unaware that law enforcement	52	29	81
	64%	36%	16%
civil remedy	37	52	89
	42%	58%	17%

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 36 month period.
Note: In 1999, 51% or our survey respondents acknowledged financial losses, but only 31% or respondents could quantify the losses.

How money was lost	Incidents w/ Quantified Losses				Lowest Reported			Highest Reported			Average Loss			Total Loss			
	1997	1998	1999	97-99	1997	1998	1999	1997	1998	1999	1997	1998	1999	1997	1998	1999	97-99
Theft of proprietary info.	21	20	23	64	$1,000	$300	$1,000	$10,000,000	$25,000,000	$25,000,000	$954,666	$1,677,000	$1,847,652	$20,048,000	$33,545,000	$42,496,000	$96,089,000
Sabotage of data or networks	14	25	27	66	$150	$400	$1,000	$1,00,000	$500,000	$1,000,000	$164,000	$86,000	$163,740	$4,285,850	$2,142,000	$4,421,000	$10,848,850
Telecom eavesdropping	8	10	10	28	$1,000	$1,000	$1,000	$100,000	$200,000	$300,000	$45,423	$56,000	$76,500	$1,181,000	$562,000	$765,000	$2,508,000
System penetration by outsider	22	19	28	69	$200	$500	$1,000	$1,500,000	$500,000	$500,000	$132,250	$86,000	$103,142	$2,911,700	$1,637,000	$2,885,000	$7,433,700
Insider abuse of Net access	55	67	81	203	$100	$500	$1,000	$100,000	$1,000,000	$3,000,000	$18,304	$56,000	$93,530	$1,006,750	$3,720,000	$7,576,000	$12,302,750
Financial fraud	26	29	27	82	$5,000	$1,000	$10,000	$2,000,000	$2,000,000	$20,000,000	$957,384	$388,000	$1,470,592	$24,892,000	$11,239,000	$39,706,000	$75,837,000
Denial of service	n/a	36	28	64	n/a	$200	$1,000	n/a	$1,000,000	$1,000,000	n/a	$77,000	$116,250	n/a	$2,787,000	$3,255,000	$6,042,000
Spoofing	4	n/a	n/a	4	$1,000	n/a	$1,000	$500,000	n/a	$1,000,000	$128,000	n/a	n/a	$512,000	n/a	n/a	$512,000
Virus	165	143	116	424	$100	$50	$1,000	$500,000	$2,000,000	$1,000,000	$75,746	$55,000	$45,465	$12,498,150	$7,874,000	$5,274,000	$25,646,150
Unauthorized insider access	22	18	25	40	$100	$1,000	$1,000	$1,200,000	$50,000,000	$1,000,000	$181,437	$2,809,000	$142,680	$3,991,605	$50,565,000	$3,567,000	$58,123,605
Telecom fraud	35	32	29	96	$300	$500	$1,000	$12,000,000	$15,000,000	$100,000	$647,437	$539,000	$26,655	$22,660,300	$17,256,000	$773,000	$40,689,300
Active wiretapping	n/a	5	1	6	n/a	$30,000	$20,000	n/a	$100,000	$20,000	n/a	$49,000	$20,000	n/a	$245,000	$20,000	$265,000
Laptop theft	160	162	150	472	$1,000	$1,000	$1,000	$1,000,000	$500,000	$1,000,000	$38,326	$32,000	$86,920	$6,132,200	$5,250,000	$13,038,000	$24,420,200
													Total Loss:	$100,119,555	$136,822,000	$123,779,000	$360,720,555

CSI/FBI 1999 Computer Crime and Security Survey
Source: Computer Security Institute

OPENING STATEMENT OF THE HONORABLE JOHN F. KERRY, RANKING MEMBER, COMMITTEE ON SMALL BUSINESS, AND A UNITED STATES SENATOR FROM MASSACHUSETTS

Senator KERRY. Thank you, Mr. Chairman, very, very much. And thank you for this particular forum and for its structure. I congratulate you on that. I think it is a terrific way to combine the input from the panel, but also to have a dialogue. I think this Committee does an excellent job of being creative in how we do our information-gathering and digesting, so I think this is a good way to do it.

Let me just say very quickly that this is a timely, fascinating topic, for reasons that everybody here understands very well. I have the pleasure of also sitting on the Commerce Committee and I sit on the subcommittee with Senator Burns, and on both the Technology and Communications Subcommittees of the Commerce Committee. So I am really having as good a time as I have had since I have been in the United States Senate learning about and watching the extraordinary entrepreneurial creativity that is taking place in this sector, which many people assure me is really only just beginning in many ways.

The disintermediation that is going to take place in the context of our economy is, I am convinced, going to be just enormous. We are already witnessing it. It will remake not everything, because consumers will always want to touch and feel and try and have a certain kind of experience in the context of their consumerism. But nevertheless, it will shape every kind of retail establishment in one way or the other, affect distribution monumentally, and most people are sharing with us the ways in which it will particularly be mostly business-to-business oriented in its impact, certainly at the earliest stages. We are seeing that.

So this particular issue in small business looms even larger in that context because most of America is small business. And the Internet offers, obviously, this remarkable democratization of sales. You can be small and new and offer up something that can compete with the old and large and big. That is really what is fascinating about it, is that it creates these new opportunities.

But obviously, one of the great restraints has been, is today, and will continue to be people's perceptions of security, of their privacy, which is another great issue we are grappling with here in the Congress. As I talk to CEOs of these companies I am convinced that they understand better than anybody, because they are in the middle of it and they are doing it with a passion, that they want this thing accessible to everybody and as available as possible; free if possible, in most contexts.

But at the same time, there is this confrontation with these other issues that we are here to talk about today. How do you keep it that accessible, and that open, and that free if people disrespect it in the way some have chosen to over the last years.

This is not just this year this has happened. I began to learn about some banks that had some rather embarrassing experiences a number of years ago and their choice was obviously not to let the world know about it, they were so embarrassed by it. So we have only now seen this surface as a kind of legitimate issue in the context we have to deal with it.

The Chairman has properly shown the number of increases of incidents. I think the White House yesterday, the White House Office of Science and Technology was quoted as saying in *Roll Call* that there may be $100 million of cost associated with this. And the professional associations say it may be as much as $250 billion worth of actual losses, which is different from cost.

So we are glad to hear from people here today. I am pleased with everybody on the panel. I particularly want to say welcome to Cisco who has been just a huge mover, player in what is happening globally, and we are delighted to have them opening a campus in Massachusetts now and engaged there.

This is something the industry will solve, in my judgment. It is something that technology itself will solve, and I think Government needs to be careful not to—we should air it. We should discuss it. But we ought to be wary of maybe rushing in with solutions. But I think that is the purpose of today's discussion.

Final comment is, I apologize that as usual around here I have about 17 different conflicts and several of them are hearings so I cannot be here for the whole thing. But my staff will be and I certainly look forward to reviewing the record and listening to the parts of the discussion I can.

Thank you, Mr. Chairman.

[The prepared statement of Senator Kerry follows:]

Prepared Statement of Senator John F. Kerry, Ranking Member
Committee on Small Business
Forum entitled "CyberCrime: Can A Small Business Protect Itself?"
Thursday, March 9, 2000

Good morning and welcome to the Committee's hearing on "CyberCrime: Can A Small Business Protect Itself?" I also would like to thank Chairman Bond for scheduling this forum, and I look forward to hearing the presentations of the panelists, as well as the discussion to follow amongst the forum participants. As we move into the new millennium, it is increasingly important that this committee examine all of the issues related to electronic commerce. Unfortunately, one of the largest issues related with e-commerce is the security of the transactions conducted over the Internet, and preventing unwanted intrusions into computer systems.

Recently, there have been a number of hearings in both the House and the Senate addressing the "next wave of computer hackers" and according to published reports, both houses are examining anti-hacking legislation and examining ways the federal government can protect its systems. While this is a worthy effort deserving of close examination, it is important that our nation recognizes the effect that recent events, and future intrusions could have on small firms.

Recent denial of service attacks against popular web sites like Yahoo! and eBay have raised concerns about the security of Internet transactions. It has also been reported that the servers of small businesses were compromised in these attacks, and served as a conduit for attacking these sites. Therefore, it is important that small businesses are aware of the hazards of not having a secure site. Not only is their proprietary information in danger, but their infrastructure could be used to harm other businesses, whether they be large or small.

Over the past ten years, there has been an increase in the number of computer-related intrusions reported by the Computer Emergency Response Team Coordination Center, an independent group sponsored by the Carnegie Mellon Software Engineering Institute. The group studies Internet security vulnerabilities, provides incident response services to sites that have been victims of attack, publishes a variety of security alerts, research security and survivability in wide-area-networked computing, and develops information designed to improve site security. In 1990, there were 252 incidents of some form of CyberCrime found by CERT. By 1999, that annual number had risen to 8,268.

Additionally, according to yesterday's *Roll Call*, the White House Office of Science and Technology estimates an annual cost of $100 million resulting from cybercrime, and the American Society for Information Science (ASIS) estimates losses at over $250 billion. These figures are both stunning and alarming, and I thank the Chairman for holding this forum to bring light to these issues. It is vital that small businesses are not left behind, and kept up to date on Internet security.

It is my hope that this forum will facilitate a larger dialogue, that small businesses will be able to pick up valuable information about keeping their electronic information secure, and I thanks the panelists for taking time out to address out forum. I also hope that the representatives of the small business associations present here today will pass on information gained today to their clients and members.

Chairman BOND. Thank you very much, Senator Kerry. I too am being pulled in 11 different directions, and with Paul Conlon on my staff and Damon with your staff we are going to conduct the business and we hope that many of our colleagues will be able to join us. But one of our colleagues who has been a real leader in discussions of e-commerce and technology for a long time is here. We are very delighted to have Senator Kerry and Senator Burns' expertise in this area.

With that, let me call on Senator Conrad Burns of Montana for his comments and insights into this.

OPENING STATEMENT OF THE HONORABLE CONRAD BURNS, A UNITED STATES SENATOR FROM MONTANA

Senator BURNS. Thank you, Mr. Chairman, and thanks for calling this hearing. I too want to congratulate you on the structure of this hearing. I am going to submit my statement for the record.

Chairman BOND. It will be accepted.

Senator BURNS. However, I want to make a couple of comments. As we look at this and what really brought us to this day of when Yahoo and eBay and e-Commerce and I think maybe a couple of trading houses were jammed, and it was not hacking as we understand it. In other words, hacking as we have always understood it is a person getting into a secure site illegally. Basically this one had to do with the enlistment of surrogate or many computers on the outside to jam the lines or to overload the system of any particular web site. That is the way I understand it.

There was not actually an illegal entry into a secure site. It was they surrounded the site where nobody else could get into it, and that is a little more disconcerting to me because the situation of hijacking other computers and other systems in order to do your work for you is troubling to us, and as we look at this situation, what it would cost small business.

The Chairman is exactly right, e-Commerce last year had a terrific year in growth. Although they only amounted to 1 percent of the retail sales totally in this country, they sent a strong message to the commerce sector of our country saying that we are a player now, and even the smallest web site can compete with the largest and the most well-established. That is an encouraging sign when we talk about commerce and the competition in the marketplace.

So this morning I look forward to the comments of our panel and our experts here. I too am pulled 11 ways but I am OK until the twelfth one is added. Thank you, Mr. Chairman.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF SENATOR CONRAD BURNS
Committee on Small Business
Forum entitled "CyberCrime: Can a Small Business Protect Itself?"
March 9, 2000

Thank you Mr. Chairman. Mr. Chairman, I would like to thank you for holding this forum on the very critical issue of Internet security and privacy facing our nation's small businesses.

I am all to familiar with this subject, as just yesterday, I held a hearing which focused on the unprecedented and apparently coordinated recent series of hacker attacks which caused some of our most popular web sites on the Internet to go dark. As you know, the list of sites that were brought down included such Internet mainstays as Amazon.com, eBay, cnn.com, e-Trade and Yahoo.

These attacks wreak havoc on businesses-big and small-across our country and around the world. It appears the hackers planned their attacks months in advance, going so far as to set up software on many servers all over the Internet that was capable of automatically flooding targeted web sites at certain predetermined times. I suppose it's no surprise that these malicious programs are called "daemons." Many of the hackers involved in theses attacks have yet to be caught, despite the coordinated efforts of our nation's top law enforcement agencies.

While no consumer data was stolen, real damage was done–especially to Internet users' confidence about the security of the systems they are using and businesses they are supporting. The nature of these attacks is particularly alarming, as they were specifically designed to disrupt electronic commerce.

The growth of electronic commerce and the Internet in general has been astounding. The number of small businesses on the Web is doubling every year, and currently over 2 million small businesses in the United States have web sites. In my home state of Montana, companies such as Vanns.com and Streaming Solutions are showing that all it takes is a great idea and hard work to reach global markets through the Internet. The e-commerce potential of the Internet still has tremendous upside.

However, the growth and reach of the Internet is a double-edged sword. Unfortunately, we now live in a world where malicious criminals can bring large parts of the nation's business community and critical information infrastructure to a grinding halt.

Given the seriousness of these attacks, we must act quickly and effectively. We need to do everything possible to foster better coordination between government and industry in protecting Internet security, make sure our national security and law enforcement agencies have the resources to do their jobs and bring our nation's criminal code up-to-date with the recent development of the Internet.

Clearly, the current level of coordination between government agencies and the private sector needs to be as seamless and effective as possible. A core component in achieving this cooperation is the continuing development of the FBI's National Infrastructure Protection Center, which was setup two years ago to deal with a range of potential attacks on the Internet.

However, I am concerned that our nation's small businesses may be getting left behind. Small Businesses are not immune from the terrors of Internet hackers. In fact, many times the repercussions caused by Internet hackers are far worse for small businesses, as they lack the financial resources and manpower that larger companies use to recover. Not only do hacker attacks cause great financial losses to many small businesses, often the business' damaged reputation to customers can be far worse. In some cases, small businesses have been forced to close their doors because of losses from cybercrime--losses unable to be recovered.

Today, the vast majority of hacker attacks are done through simply downloading pre-existing programs from hacker sites on the web and using them to accomplish destructive aims. Rather than stemming from misdirected teenage rebellion, current attacks are often engaged in by adults who want to inflict the most damage possible. The destruction of data belonging to innocent individuals and businesses is no less a crime than property destruction of the more traditional type. In fact, it can in many cases be far worse.

Although we have seen promising efforts in the area of increased security on the Internet, more needs to be done for small businesses. Many times we recognize the need to protect and help large companies, while overlooking the small business community. We can no longer do this.

We are fortunate to have small business owners, along with government and industry experts in the field of Internet security with us today. I look forward to hearing from each of you in addressing these matters of critical importance to the continued secure development of e-commerce and the Internet. Thank you.

Chairman BOND. Thank you, Senator Burns.

Now let us get down to business. First we welcome Ms. Joan Neptune, general manager, LC Communications of Davie, Florida; one who can speak to us with great personal experience in this area. Ms. Neptune, welcome.

STATEMENT OF JOAN NEPTUNE, GENERAL MANAGER, LC COMMUNICATIONS, DAVIE, FLORIDA

Ms. NEPTUNE. Thank you very much for having me here today. In 1996, I was executive vice president of a small ISP located in south Florida. When I tell this story please remember that it was in the beginning days of the Internet and technology is not what it is today. But at that time we were the victim of a CyberCrime that eventually had a devastating financial impact on the company.

We offered many services. We offer all different types of access, web hosting, web development. We were connected to the customers through the public telephone network and into the Internet through a backbone provider, and of course, we had a billing platform where the customer information was. Plus about 80 percent of our customers did use credit card billing, so all the credit card information and other secure information about their passwords and logins were located on the billing server.

One day in the early morning hours, miraculously the login and password file that you use to actually get into the Internet every time you dial in, was missing. We immediately went to our backup tapes, installed the backup of the file and then looked into the log files to see what had happened. We had determined that an unauthorized user had come in through a computer terminal that was left on, used a terminal simulator program so that they were actually looking like they were the operator of the terminal at the time.

We instituted new procedures. A couple of weeks later the same thing happened. When we put the backup in, a few days passed and we received an e-mail from them saying that they were very upset and the reason that they had done this was because we had shut down an unauthorized chat room. We had chat rooms as one of our services, but this was unauthorized. They were using a lot of bandwidth. They were blocking our customers from accessing the Net.

We decided not to put the unauthorized chat room back on. We installed new procedures, ordered new firewalls. We did have other firewalls, but the system was increasing over time and new technologies were coming out daily.

A couple of weeks passed and again the system crashed, but this time they also deleted all of our customer web sites, hosting sites, et cetera. Of course as luck would have it, the backup was corrupted, so it was not a good backup and about 10 percent of the web sites were lost which we did have to redevelop on-site.

A few days passed and we got an e-mail saying that they were not kidding around, and they had copies of our customers credit cards, and they wanted $30,000 otherwise they would sell these credit cards, notify our customers, et cetera. At that point we began to take them very seriously and contacted our corporate attorneys who referred us to the Secret Service through contacts, because the Secret Service was the agency that handled credit card fraud.

It was very fortunate at the time that hacking was just coming into the limelight and the Secret Service was looking for a test case and looking to develop procedures to track people on the Internet. The Secret Service did come in. They were very wonderful. They lived day and night at our office.

While we were sending e-mails back and forth to the hackers, which were passed by the Secret Service psychologist to kind of peg them in and develop a rapport, we also had to shut down a lot of our services like telenetting, chat rooms, et cetera, to our customer base because we needed to limit the access of the hackers. We could not notify our customer base and we could not notify most of our employees because the Secret Service did not want anybody to get wind of the investigation that was going on.

About a month passed and finally a set up, a plan was developed and they wanted us to send $30,000 hidden in a book, overnight special delivery. By that time we had tracked the hackers back to Germany through the telecommunications industry. We were able to find the login files to find the telephone number that they had originated their access into our system from, tracked it back to an MCI long distance switch in New England, and then MCI helped track it back to access numbers in Germany.

So the Secret Service had also gotten the German local authorities involved in this. The Secret Service flew over to Germany, waited with the German police at the dropoff point and a young gentleman picked it up. Of course, he was not the culprit. He was only instructed to pick it up, drop it at another destination. This went on through four different dropoff points. Finally, they found the gentleman, who turned out to be a college student who had spent his college money that his parents had given him and he needed this $30,000 to replace the money.

The Secret Service had no authority in Germany so the case was turned over to the local authorities, and he was charged with a minor crime, which I cannot really recall exactly what it was called. About 6, 7 months later he went to trial. His family was very influential. He got 14 months probation and a slap on the wrist.

Back on the homefront though, this cost us very much more than a slap on the wrist. Obviously, after the third hacking incident our customers were not happy. There was a lot of competition in the Internet involvement, as there is today, and they simply went to other carriers. Then when our services were curtailed, they went to other carriers. The money that we had earmarked for expansion instead went to putting in firewalls. Eventually we had to, because they did find the credit card numbers on the hacker's hard drive, we had to notify all of our customers in the end that their credit cards could have been compromised.

So the cancellation rates went crazy and we were never able to come back from this devastating experience. Our momentum in the marketplace was lost. Our reputation was ruined in the marketplace. We had to expend about $500,000 in expenses of which we only received about $135,000 back from insurance. So all around it was a death sentence.

The only good thing, and I would like to underline here, was how wonderful the Secret Service was to us. They really worked day

and night and saved the company at that point. I thank them and I thank you for having me here today.

[The prepared statement of Ms. Neptune follows:]

Prepared Statement of Joan Neptune, General Manager
LC Communications, Davie, Florida
before the Senate Committee on Small Business
Forum entitled "CyberCrime: Can a Small Business Protect Itself?"
March 9, 2000

My name is Joan Neptune and in 1996 I was Executive Vice President and part owner/founder of a small internet start-up company located in South Florida. During that year, the Company was the target of a CyberCrime known as hacking and I have been asked to talk to you today about the financial and operational impact this CyberCrime ultimately had on the business.

To understand the impact of the crime, allow me to give you a brief background on the Company. As I mentioned previously, the Company was an Internet Service provider offering dial up and dedicated access to residential and business customers, including value added services such as email, daily news, weather, and chat rooms. We also offered a full range of web development, co-location and site hosting services. Our equipment consisted of an extensive network of modems, routers, and servers connected to the customers through a large telecommunications infrastructure supplied basically by the local phone companies through the public telephone network. Billing was done on site through a company implemented billing platform that contained complete customer billing, password, and credit card information. At the time, the Company had a customer base of approximately 10,000 individual and business accounts, 50 reseller/agent accounts, plus numerous trade associations and retail agreements with outlet chains throughout South Florida. Of these accounts, 80% were billed directly through credit cards.

The first sign of a problem occurred in the early morning hours sometime in June 1996. All of the customer Internet connections were disconnected and no customers could establish new connections. It was discovered that an unauthorized user had broken the system administration passwords allowing the user to delete files containing the user passwords and logins. In addition, they had gained access through a customer service terminal that had been left on, and through a terminal simulator program had become, in essence, the terminal operator. The Company immediately restored the system by installing a backup tape containing the deleted information, changed the system passwords, and instituted strict procedures about signing off individual computer terminals.

A few weeks later, the same problem occurred. When the system was restored, we received an email from the hackers stating that the reason they had entered our system was because the Company had shut down an "unauthorized" chat room. They wanted it immediately restored and available for their use at all times. The Company refused to restore the chat room as it was using enormous amounts of bandwidth and blocking our customers from accessing the Internet.

At this point, several days passed before the "hackers" again deleted the login and password files. In addition, this time they also deleted the customer web sites and destroyed the customer email files. Once again the Company installed backup tapes to reinstitute the system, but the backup

tapes of the customer web sites was corrupted and the Company had to revert to a week old tapes of that material. To protect the system in the future, we immediately ordered and installed a more secure "firewall", which basically put the system administration files behind a "wall" of security at a cost of approximately $20,000. During the 4 days it took to install the firewall, the Company had technicians constantly monitoring the system 24 hours a day and also incurred enormous amounts of overtime to recreate the lost customer web sites.

Approximately one week later, the Company received an email stating that they, the "hackers", were not "kidding around". They had a complete list of our customers' credit card numbers and would not hesitate to use them, publish them, and email our customers directly with threats concerning the use of their credit cards. They demanded $30,000 and would contact us shortly. At this point, although the Company felt there was only a small possibility that the hackers actually were in possession of credit card information, we took their threats seriously. While the Company initiated an internal investigation, we contacted our corporate attorneys for advice concerning the involvement of law enforcement agencies.

The Company learned that credit card fraud and theft was under the auspices of and the responsibility of the Secret Service. Our attorneys located a contact at that agency and a meeting was scheduled for the following day. As it turned out, CyberCrime was just entering into the limelight of media attention and the Secret Service was looking for a "test" case. For the next month, the Secret Service literally lived at our offices. We managed to track the hacker access to four other Internet Services Providers, including IBM.net, only to learn that their systems had also been compromised on the same days.

During that month, with the guidance of the Secret Service, we kept the hackers at bay with a series of emails allegedly setting up a plan for the delivery of the money. At the same time, many of the staff at the Company had numerous years of operational experience in the telecommunications industry and they used that experience to track the telephone access numbers the hackers had used to an MCI switch located in New England. The Secret Service then used these same tracking procedures and "enlisted" the help of MCI to further track the individuals to their point of origination in the public telephone network. The culprits had originated outside of the United States in Germany and the agents contacted the local German police for assistance.

In the meantime, the hackers had instructed us to send the money, hidden inside a book, for overnight delivery to a post office box in Germany. The Secret Service fronted the money, set up step by step contact with the delivery company at every point on the route, flew over to Germany, combined forces with the German police, and established surveillance of the post office box. A young gentleman eventually picked up the package but only had instructions to deliver the package to another address. This went on through four additional drop off points and deliveries until the responsible party was located. The hacker turned out to be a college student in Germany who had spent the money his parents had given him for college. In his desperation, he had devised this plan to replace his college funds. The Secret Service had no jurisdiction in Germany and had to leave the matter in the hands of local law enforcement agencies. The student was charged with a minor crime and ultimately sentenced to 14 months probation-no fines and no restitution.

The impact on the Company was far greater than the sentence. At the time of the CyberCrime, the Internet was in its infancy. The industry and service opportunities were not yet clearly defined. Competition for customers was enormous. Capital outlays for equipment, software, telephone circuits and personnel were hundreds of times in excess of revenue streams while interest from financing institutions was minimal. At the beginning of the hacking incident, the customer base was only slightly inconvenienced and cancellation rates were only slightly above normal. However, by the third incident, customers no longer cared about the reasons they couldn't use their Internet service and went to other Internet Service providers. Customers who hosted their web sites at the Company were losing business and changed their service to other web hosting companies.

Once the Secret Service joined the investigation, we were instructed not to let our customers or employees know anything that was taking place for fear the hackers would find out about the involvement of law enforcement. At that point, the Secret Service also was not sure if any employees were involved, so only employees integral to the investigation knew any details. In addition, the Company had to restrict its service offerings, per the instructions of the Secret Service, to limit illegal entry by the hackers. Customer and employee confusion and dissatisfaction were the norm. The result was enormous amounts of overtime in the customer service and operations departments, high cancellations rates, lack of new sales, high employee turnover, and enormous capital expenditures for salaries as well as fraud software/hardware. Money was also lost on advertising that could not be cancelled, new recruitment costs, and payment of leases for equipment that was no longer being used due to the high cancellation rate. These monies had been allocated for expansion of service areas and service offerings, so the future growth of the Company, necessary for profitability, was delayed indefinitely.

After the arrest was made in Germany, the Company also had to notify each customer that their credit card number might have been jeopardized. The result was even higher cancellation rates and a severely damaged reputation in the consumer marketplace. The Company lost its momentum and growth and could never fully recover. Although we had insurance coverage for loss of business income, the estimated losses and expenses from this CyberCrime were approximately $500,000 while insurance recovery was $135,000. The hacker received a "slap on the wrist" while the Company received a death sentence. The Company was eventually sold in 1999 at a considerable loss to the original investors and approximately 100 employees lost their means of support. The only good thing to happen during this time was the positive support and involvement of the Secret Service. I thank them and I thank you for your time.

Chairman BOND. Ms. Neptune, that is a very scary tale and that is also a wonderful introduction for our next panelist, Special Agent Mary Riley, assistant to the special agent in charge of the Financial Crimes Division of the United States Secret Service in Washington.

Ms. Riley, welcome.

STATEMENT OF MARY RILEY, SPECIAL AGENT, ASSISTANT TO THE SPECIAL AGENT IN CHARGE, FINANCIAL CRIMES DIVISION/ELECTRONIC CRIMES BRANCH, UNITED STATES SECRET SERVICE, WASHINGTON, D.C.

Ms. RILEY. Thank you very much, Mr. Chairman. Good morning.

Within the Secret Service we have been working these network intrusion type investigations—Ms. Neptune outlined one of the perfect examples of that this morning—since about 1987. The focus of our efforts and in an effort to avoid duplication or unorganized activity between law enforcement agencies, we have tried very hard to focus our investigative efforts in the areas of financial institutions and telecommunications networks, such as that that Ms. Neptune described this morning.

It has allowed us to really train our agents and give them an expertise in a smaller number of networks so that as they do respond to victim companies they have the ability to understand the types of questions to ask, the types of investigative techniques to bring forward, and keep that germane to a smaller segment of industry and allow the expertise to work through the investigations.

One of the most important things that we have seen in working with victims in these types of cases is that we as law enforcement have got to take on a great deal of responsibility in protecting the victim throughout the investigation. We have to ensure that the activities that we have to deploy throughout the investigation do not cause greater harm to the victim than the original hacking activity or the criminal activity that brought them to our attention in the first place.

For example, within the investigation that was outlined for you this morning, when 11,000 credit card numbers were identified as having been potentially compromised not only would there be harm in notifying a broad sector in some blanket notification that those numbers could have been potentially compromised. At that point we had a lot of threats but no confirmation initially that this information had actually been stolen. It was simply a threat to try to entice the victim in this case to provide the $30,000 or the open access into their network. They were using any type of threat that they could.

What we did from our angle was, because of our experience within the credit card industry, for example, we have been working extensively with that industry for the last 15 years, we were able to take the information provided to us by the victim and take that information to the credit card issuers saying, these are potentially compromised numbers. Let us keep that in that realm initially. Let us not go out and notify every customer out there who may be somewhat skeptical about using credit cards on the Internet in the first place or dealing within the electronic commerce arena. Let us

try to keep this in perspective. Let us make sure that we are only acting on known facts.

Threats have got to be treated as such until we can provide confirmation there. The credit card industry responded admirably. They were able to take all 11,000 numbers, notify the issuers to flag those accounts in the event fraud activity did occur, but keep it within that realm until we could provide further confirmation through the activity in Germany that was later done in the search warrants at the suspect's residence.

Another example of that same type of activity occurred when we had a network intrusion into a telecommunications company in Boston. The telecommunications company that provided services to the public was, of course, one of the primary victims. But a smaller business that was affected there was the company that actually manufactured the switch that was affected. Their reputation was on the line immediately once that switch was compromised.

The first thing that we did in that investigation, once we identified the methods used by the suspects in that case, was contact the manufacturer of the switch and also give them the opportunity to notify their customers themselves of the compromised activity and the work that they were doing with law enforcement to provide a fix.

The United States Attorneys Office was then incredibly responsive and agreed to give us the time—us meaning law enforcement and industry, to ensure that the company had the opportunity to work with their customers, develop patches that would allow the compromised activity to be discontinued completely, and ensure that at no time did we release any information about the case that could have caused that victim to suffer further harm as a result of our actions. All prosecution, for example, in that particular case was withheld until the fixes were put into place by the small company that manufactured the switches there.

We find that it is incredibly important to ensure in all of our partnerships with industry and with other law enforcement agencies that we take the benefit of our experience, that every time we learn a new lesson in dealing with industry victims and in dealing with the types of vulnerabilities out there, that we are very candid with our industry partners so that we can learn from these past experiences. We would like to support entirely the prevention techniques that are being deployed by industry, such as those outlined in Mr. Farnsworth's written statement where he outlines some very effective prevention techniques that industry can use to keep these types of events from happening to other victims.

We would like to continue to share the information that we have picked up from the industry, from the different types of suspect interviews that we have done, and the technical reviews of the actual hacking activity and just continue to get that out to industry and to any agencies and companies that are affected by these types of cases so that we can learn from the past experience and hopefully deploy more prevention techniques, as you well mentioned, that technology can work to solve this problem by taking advantage of the information we have.

Thank you for the opportunity.

[The prepared statement of Ms. Riley follows:]

Department of Treasury

U.S. SECRET SERVICE

Testimony of Mary K. Riley

Assistant to the Special Agent in Charge

Financial Crimes Division/Electronic Crimes Branch

U.S. Secret Service

For Presentation to the

Committee on Small Business

March 9, 2000

MR. CHAIRMAN, MEMBERS OF THE COMMITTE, THANK YOU FOR THE OPPORTUNITY TO ADDRESS THIS COMMITTEE CONCERNING THE SUBJECT OF HIGH TECH CRIME AS IT RELATES TO THE SMALL BUSINESS COMMUNITY AND THE SECRET SERVICE'S EFFORTS TO COMBAT THIS PROBLEM.

MY NAME IS MARY RILEY, AND I AM THE ASSISTANT TO THE SPECIAL AGENT IN CHARGE OF THE ELECTRONIC CRIMES BRANCH FOR THE UNITED STATES SECRET SERVICE. THE BRANCH IS RESPONSIBLE FOR THE CASE COORDINATION OF ALL TELECOMMUNICATION AND COMPUTER NETWORK INVESTIGATIONS CONDUCTED BY THE SECRET SERVICE DOMESTIC AND INTERNATIONAL FIELD OFFICES. THE BRANCH ALSO COORDINATES THE FORENSIC ANALYSIS OF COMPUTER AND TELECOMMUNICATIONS EQUIPMENT SEIZED AS EVIDENCE IN ALL INVESTIGATIONS THROUGH A TEAM OF 110 SPECIAL AGENTS TRAINED AS EXPERTS IN THE EXAMINATION OF ELECTRONIC EVIDENCE.

THE SECRET SERVICE HAS TAKEN PROACTIVE POSITIONS IN IDENTIFYING FRAUD AS IT OCCURS THROUGHOUT THE FINANCIAL, ELECTRONIC COMMERCE AND TELECOMMUNICATIONS INDUSTRIES. THE GROWTH AND EVOLUTION OF THE INTERNET HAS PROVIDED NUMEROUS COMMERCIAL AND FINANCIAL OPPORTUNITIES, SPECIFICALLY IN THE AREAS OF ELECTRONIC COMMERCE. WITH THE

EXPONENTIAL GROWTH OF THE NATIONAL INFORMATION INFRASTRUCTURE, THE SAME TYPE OF GROWTH CAN BE EXPECTED AND IS OCCURRING IN THE AREAS OF HIGH TECHNOLOGY CRIME ON A GLOBAL BASIS. TECHNOLOGICAL ENHANCEMENTS TO WIRELESS COMMUNICATIONS AND THE IMPROVEMENTS IN TRANSPORTATION SYSTEMS HAVE CREATED AN ENVIRONMENT IN WHICH STATE AND INTERNATIONAL BORDERS BECOME JURISDICTIONAL OBSTACLES FOR LAW ENFORCEMENT AGENCIES, AND BECOME SYMBOLIC OBSTACLES TO CRIMINALS. THIS IN CONJUNCTION WITH THE EASE WITH WHICH ANYONE CAN EITHER COUNTERFEIT OR FRAUDULENTLY OBTAIN FALSE IDENTITY AND TRAVEL DOCUMENTS, FURTHER MAGNIFIES THE CHALLENGES POSED TO THE ENTIRE LAW ENFORCEMENT COMMUNITY.

AT THIS TIME, A GREAT DEAL OF ATTENTION IS PAID TO THE NEED TO CHANGE THE TRADITIONAL METHODS OF LAW ENFORCEMENT PRACTICES IN THE INTERNATIONAL ENVIRONMENT. THROUGH SOLID PARTNERSHIPS DEVELOPED BY OUR INTERNATIONAL FIELD OFFICES, INCLUDING JOINT TRAINING INITIATIVES WITH LAW ENFORCEMENT AND INDUSTRY, WORKING THROUGH GEOGRAPHIC BOUNDARIES HAVE BROUGHT SIGNIFICANT HIGH-TECH INVESTIGATIONS TO SUCCESSFUL CONCLUSIONS.

TITLE 18 USC 1029 WAS AMENDED TWICE IN 1994 AND 1998 TO INCLUDE SIGNIFICANT CHANGES RELATED TO COMPROMISES OF THE TELECOMMUNICATIONS SYSTEM. THE SECRET SERVICE HAS TAKEN AN EXTREMELY PROACTIVE ROLE IN THE INVESTIGATION OF TELECOMMUNICATIONS FRAUD/INTRUSION ACTIVITY AND THE EDUCATION OF INDUSTRY REPRESENTATIVES AS TO THE VULNERABILITIES. AS SUCH, THE SECRET SERVICE IS RECOGNIZED AS THE LEADER IN THE INVESTIGATION OF THIS SPECIFIC TYPE OF ACCESS DEVICE FRAUD AND ROUTINELY PROVIDES TRAINING TO LAW ENFORCEMENT AND INDUSTRY PERSONNEL AT ALL LEVELS. THESE TYPES OF INVESTIGATIONS, IN MANY INSTANCES, ACT AS A NEXUS TO OTHER CRIMINAL ENTERPRISES SUCH AS ACCESS DEVICE FRAUD, COUNTERFEITING, MONEY LAUNDERING, AND THE TRAFFICKING OF NARCOTICS.

IN 1986, TITLE 18 WAS REVISED TO EMPOWER THE SECRET SERVICE TO INVESTIGATE FRAUD AND RELATED CRIMINAL ACTIVITIES INVOLVING COMPUTERS. TITLE 18 USC 1030, CONTINUES TO EVOLVE AS COMPUTER NETWORKS AND CRIMINAL ACTIVITY ASSOCIATED WITH NETWORK VULNERABILITIES BECOME MORE COMPLEX. THE SECRET SERVICE STRIVES TO PROVIDE INVESTIGATIVE FOCUS ON THE TELECOMMUNICATIONS AND BANKING AND FINANCE SECTORS IN

COMPUTER FRAUD INVESTIGATIONS. THAT FOCUS HAS PROVED TO BE AN ASSET IN THE EFFECTIVENESS OF SECRET SERVICE INVESTIGATIONS AND THE ABILITY TO TRAIN AND EQUIP FIELD OFFICES TO ADDRESS SPECIFIC HIGH-TECH INVESTIGATIONS.

THE INTERNATIONAL MARKETPLACE IS QUICKLY MOVING TOWARD A RELIANCE ON ELECTRONIC COMMERCE, AND LAW ENFORCEMENT MUST BE PREPARED TO DO OUR PART TO PROTECT THE INTEGRITY OF THE SYSTEM AND TAKE ACTION AGAINST THOSE WHO TARGET IT FOR CRIMINAL ACTIVITY. THE PROTECTION OF COMMUNICATIONS SYSTEMS AND NETWORKS DEDICATED TO ELECTRONIC COMMERCE LEADS TO REDUCTIONS IN COSTS THAT WOULD OTHERWISE BE PASSED ON TO CONSUMERS WHEN MERCHANTS AND ONLINE PROVIDERS ARE VICTIMIZED BY FRAUDULENT ACTIVITY.

THE CRIMINAL ACTIVITY ASSOCIATED WITH COMPUTER NETWORKS AND ELECTRONIC COMMERCE IS NOT EXCLUSIVE TO SPECIFIC SEGMENTS OF INDUSTRY OR DEPENDENT ON A VOLUME OF BUSINESS. RECENTLY, OUR FIELD OFFICES CONDUCTED INVESTIGATIONS INVOLVING VICTIMS RANGING FROM MULTI-NATIONAL FINANCIAL INSTITUTIONS TO SMALL MERCHANTS CONDUCTING BUSINESS THROUGH THE INTERNET. THE INVESTIGATIVE CHALLENGES ARE

THE SAME REGARDLESS OF THE SPECIFICS OF THE VICTIM COMPANIES.

TO BETTER PREPARE OUR AGENCY TO RESPOND TO AND PREVENT ATTACKS ON OUR EVOLVING ELECTRONIC PAYMENT SYSTEMS, THE SECRET SERVICE HAS TAKEN A DYNAMIC APPROACH TO TRAINING OUR AGENTS AND OUR COUNTERPARTS THROUGH STATE-OF-THE-ART COMPUTER-BASED TRAINING SYSTEMS. HIGH-TECH INVESTIGATIVE TRAINING IS BEING CONDUCTED WITH THE GOAL OF KEEPING LAW ENFORCEMENT CURRENT WITH EFFECTIVE INVESTIGATIVE TECHNIQUES THAT CAN BE UPDATED AS QUICKLY AS TECHNOLOGY ADVANCES. THE SECRET SERVICE, THROUGH ITS ESTABLISHED PARTNERSHIPS WITH INDUSTRY REPRESENTATIVES, HAS COLLECTED A LIBRARY OF EXISTING COMPUTER-BASED TRAINING PROGRAMS FROM THE TELECOMMUNICATIONS, FINANCIAL AND COMPUTER NETWORK INDUSTRY REPRESENTATIVES. WITH THESE PROGRAMS AS THE BASELINE, TRAINING MATERIAL IS ADDED TO EDUCATE STUDENTS IN LAW ENFORCEMENT METHODS AND IDENTIFICATION OF INVESTIGATIVE TOOLS, PAST CRIMINAL METHODS OF INTRUSION AND/OR COMPROMISE.

AS THE MARKET PENETRATION FOR COMPUTER EQUIPMENT IN THE HANDS OF THE GENERAL PUBLIC INCREASES EVERY DAY, AND THE

INTERNET CONTINUES WITH A GROWTH RATE OF OVER 100 PERCENT, IT HAS TO BE ANTICIPATED THAT THE CRIMINAL ELEMENT WILL UTILIZE THESE TOOLS AT THE SAME LEVELS. THE SECRET SERVICE HAS PLACED AN EMPHASIS ON THE DYNAMIC GROWTH OF OUR ELECTRONIC CRIMES SPECIAL AGENT PROGRAM (ECSAP) AS AN ESSENTIAL COMPONENT OF THE INVESTIGATIVE AND PROTECTIVE MISSIONS OF THE SECRET SERVICE. THE ECSAP PROGRAM, CONSISTING OF HIGHLY TRAINED SPECIAL AGENTS QUALIFIED AS EXPERTS IN THE FORENSIC EXAMINATION OF ELECTRONIC EVIDENCE, ARE ASSIGNED TO NEARLY ALL SECRET SERVICE FIELD OFFICES. THE PROGRAM HAS EXPANDED TO INCLUDE OPERATIONAL ASPECTS SUCH AS TECHNICAL GUIDANCE IN SEARCH WARRANT PREPARATION AND EXECUTION, EDUCATIONAL PRESENTATIONS AND TECHNICAL ADVICE TO PUBLIC AND PRIVATE SECTOR ORGANIZATIONS. AGENTS ASSIGNED TO THIS PROGRAM ARE ALSO TRAINED TO EXAMINE THE VARIETY OF ELECTRONIC EVIDENCE SEIZED IN TODAY'S CRIMINAL INVESTIGATIONS TO INCLUDE TELECOMMUNICATIONS DEVICES, ELECTRONIC ORGANIZERS, SCANNERS, AND ANY OTHER DEVICES MANUFACTURED TO INTERCEPT OR DUPLICATE TELECOMMUNICATIONS SERVICES.

THE SECRET SERVICE HAS ACHIEVED SUCCESS THROUGH A CONSISTENT PROCESS OF AGGRESSIVE, PRO-ACTIVE INVESTIGATIONS,

IDENTIFICATION OF SYSTEMIC WEAKNESSES, AND PARTNERSHIPS WITH INDUSTRY AT ALL LEVELS TO ADOPT TECHNOLOGICAL AND PROCEDURAL SOLUTIONS TO COMBAT IDENTIFIED VULNERABILITIES. THE SMALL BUSINESS COMMUNITY IS AT THE FOREFRONT TO BENEFIT FROM THE GROWTH OF ELECTRONIC COMMERCE AND, DUE TO THE PATTERNS OF HIGH TECH CRIMINAL ACTIVITY, FACES THE THREAT OF COMPROMISE ACTIVITY FOCUSSED ON THEIR NETWORKS.

THE TOOLS AND INVESTIGATIVE EXPERTISE HIGHLIGHTED BY THE SECRET SERVICE ARE INTENDED TO SERVE AS THE CORNERSTONE OF SUCCESSFUL PARTNERSHIPS WITH THE SMALL BUSINESS COMMUNITY TO COMBAT HIGH TECH CRIME.

THIS CONCLUDES MY PREPARED STATEMENT. I WOULD HAPPY TO ANSWER ANY QUESTIONS THAT YOU OR ANY OTHER MEMBER OF THE COMMITTEE MAY HAVE. THANK YOU.

Chairman BOND. Thank you very much, Ms. Riley.

Mr. Scott Charney, partner of PricewaterhouseCoopers LLP in Washington, D.C.

Welcome, Mr. Charney.

STATEMENT OF SCOTT CHARNEY, PARTNER, PRICEWATERHOUSECOOPERS LLP, WASHINGTON, D.C.

Mr. CHARNEY. Thank you. Thank you for inviting me here.

First I would like to say something about these statistics, which is that they probably under-report and under-represent the scope of the problem. The reason for that is that what you see from the CERT team and from the Computer Security Institute are reports of people who have detected and reported computer crime. It has been widely viewed by experts that most computer crimes are neither detected nor reported. Of course, it was always hard to prove that. How do you prove what someone does not know?

Well, fortunately the Defense Department did a controlled study. They attacked their own machines. They attacked 38,000 of them and they got in 65 percent of the time, 24,700 successful penetrations. But here is the really interesting statistic. They then went to the system administrators and said, how many intrusions have you detected, and the answer was, 988 out of 24,700. Basically a detection rate of 4 percent.

So then the next question was, how many of these system administrators reported the intrusions to DISA, the Defense Information Systems Agency, and the answer to that was 267; roughly 27 percent reporting rate. This is in an agency with mandatory reporting and a staff that if they know anything, it is follow orders.

So one of the things that we learned from these statistics is, they probably do not fully represent the problem. It is interesting, if you come back to Senator Burns' comments about the denial of service attacks, one of the things about a denial of service attack is, you know it happened. Your system goes down. It is easy to detect.

But other computer crimes attack the confidentiality and integrity of information. Those crimes are very hard to detect. It is somewhat interesting, as a person now in the private sector I will go to a company and say, you need to deploy computer security and they will say, "Well, we have never been attacked." And I ask, "How do you know?" And they respond, "Well, we have never seen anything go wrong."

And I ask, "Well, if I steal your car, how do you know?" And they say, "Well, my car is gone." And I ask, "If I steal your customer list how do you know?" They respond, "My customer list is—oh, no, I would still have it, would I not?" That is right. A copy has been taken, not the original. The original remains intact. So those kinds of crime are much harder to detect.

There are, of course, increasingly, preventive steps that companies can take, and some of these involve intrusion detection systems, or computer anomaly detection systems using the power of the computer to look for behavior that we know is bad.

But there are a couple of problems here. One is that the technology is not yet very mature, only it is getting better. The second thing is, how do you detect abuse in a computer network? You watch what people are doing. You monitor their activities. You see

when they log on and log off. You watch their activities on the network to see what kinds of information they are accessing.

In the context of computer security, these techniques equal surveillance. So now you run into some very serious privacy issues. How do you monitor what is going on on networks to figure out when people are abusing them without at the same time monitoring lots of innocuous activity, or activity that looks suspicious but later proves to be innocuous, and how do you protect the privacy of Americans using the Net? So needless to say, these are very complicated issues.

I would add to that, a particular problem for small business, which is the technology is changing very, very rapidly. As a result of that, each time the technology changes it costs considerable money to upgrade to the newest and greatest technology. At the same time, with each new technology comes a new set of vulnerabilities. So when people migrate from one operating system to the next, they get the vulnerabilities of this new operating system. That means that businesses have to be ever vigilant, constantly testing their systems, mapping their networks, seeing who is connected, looking for vulnerabilities, educating their users, looking for fraud.

The difficulty is, for large companies this can be very expensive. For smaller companies, where are they going to get the money to do it? To the extent they have some sort of IT budget, they are spending that budget to create opportunity; security is often viewed as a loss center as opposed to a business enabler. So it is very difficult for them to allocate their resources in a way that allows them to devote significant attention to computer security.

I will leave you with one other problem along the same lines, which is where do small businesses get the talent to deploy their computer security? There are different statistics on this. One comes from Congressmen Wolf and Moran when they talked to the Partnership on Critical Infrastructure Security, an industry group looking at security. Their number was 12. Georgia State University tells me it is 9. But whether 12 or 9, that is the number of people in the United States who graduated with a Ph.D. in computer science last year. Six of them went to industry, three of them went to Government, some went back to their home country. None of them went into academia.

So if you look at a model that we need greater computer security and we want this generation of experts to teach the next generation, that is not happening. And when a small business goes out and says, I need a system administrator who really understands technology and they are competing with the big companies of the world, it is going to be very hard for them.

Thank you.

[The prepared statement of Mr. Charney follows:]

Scott Charney
Partner, PricewaterhouseCoopers LLP
Statement before the Committee on Small Business
March 9, 2000

I would like to thank the Committee for inviting me to speak on cybercrime and the challenges it poses to small businesses. As you know, it is difficult to quantify the computer crime problem. Public reports regarding the cost of computer crime have varied widely, in part because there are no truly reliable figures to cite. The reason for this is threefold. First, there is no commonly accepted definition of a computer crime; thus, it is unclear whether certain criminal activity should be included, or excluded, from computer crime statistics. Second, for a variety of reasons discussed below, most computer crimes are still not reported. Third, even when such crimes are reported, they are not reported to any central authority for compilation.

Let me first address the definitional problem. Although computer crime definitions may differ, it is easy to define what it is not: it is not every crime committed with a computer. For example, if someone steals a telephone access code and makes a long distance call, the code he has stolen is checked by a computer before the call is processed. Even so, it is more appropriate to treat this case as "toll fraud," not computer crime. While this example may seem straightforward, many cases cannot be so neatly categorized. For example, a cashier who steals a ten-dollar bill from a cash drawer is embezzling. A cashier who writes a computer program to automatically pad the invoices of a large number of accounts may also be embezzling, but both committing and prosecuting this offense may require a working knowledge of computer applications. Thus, such a crime may reasonably be characterized as a computer offense.

From a broad perspective, there are three discrete roles that computers may play in a criminal case. First, a computer can be the target of the offense. This occurs when the actor's conduct is designed to steal information from, or cause damage to, a computer or computer network. I generally refer to these as "CIA" offenses, which means the offense impairs the confidentiality (C), integrity (I), or availability (A) of a computer system or its data. This construct comes from the Guidelines for the Security of Information Systems, issued by the Organization for Economic Cooperation and Development (OECD) in Paris, France, and it provides a helpful framework for thinking about traditional computer crime. The recent Distributed Denial of Service attack was a traditional computer crime: an attack on availability.

Second, a computer can be a tool used to facilitate a traditional offense, such as in the embezzlement described above. For small businesses accepting credit card payments over the Web, for example, the Internet may facilitate fraudulent transactions previously conducted in person or over telephone lines. Internet crimes may be more difficult to investigate, however, because the transactions are faceless and the Internet, unlike the traditional telecommunications network, does not provide for traceability. Put another way, it may be impossible to trace the fraudulent activity back to its source.

Finally, a computer may be incidental to an offense, but still significant for litigation or law enforcement purposes. Evidence is now frequently in electronic form, raising difficult computer forensics issues, such as how to recover robustly encrypted data.

Whatever definition one chooses, however, it is clear that the computer crime problem is growing. Annual surveys by the Computer Security Institute (CSI) and statistics provided by the Computer Emergency Response Team (CERT) at Carnegie Mellon University suggest that the growth of computer crime mirrors the growth of the Internet. And as the latter has been phenomenal, so has the former. For example, CSI's 1999 survey indicated that "system penetration by outsiders increased for the third year in a row: 30% of respondents reported intrusions." Additionally, "unauthorized access by insiders also rose for the third straight year; 55% of respondents reported such incidents."

These statistical reports, however, may only reveal the tip of the iceberg, for it remains generally accepted that most victims of computer offenses do not report intrusions, either to law enforcement or anywhere else. The reasons for this have been and remain varied, and some of them are, from a business perspective, understandable. Some computer offenses are simply too minor to merit reporting to CERT or to law enforcement. Many of these involve theft of computer time (e.g., workers composing personal correspondence on company computers) or other relatively minor offenses best handled by a company's or agency's internal mechanisms.

In other cases, victim companies fear the bad publicity that may accompany a public report of the intrusion, and the effect that such bad publicity may have on investor confidence. For example, in 1991, one bank officer reported to me that when his bank went public with an attack on their electronic mail system and prosecuted the intruder, the end result, notwithstanding bank assurances that accounts were never at risk, was a long line of depositors waiting to withdraw their money. Ironically, he reported, most customers took their accounts to a bank down the street running the same vulnerable software. He could only speculate that this bank had also been penetrated, but had not publicized that fact. This individual candidly admitted he would never report another intrusion publicly for fear of the repercussions. These unreasonable consequences present huge challenges to both industry leaders and government representatives who hope to change public and corporate understanding and attitudes about computer crime.

Third, victim companies often fear that a public exposure of their vulnerabilities may result in further attacks against their systems, especially if patches are unavailable or have not yet been applied.

Historically, such business concerns have discouraged reporting to law enforcement, and thus important computer crimes may have gone uninvestigated. A survey conducted by WarRoom Research in 1996 asked respondents: "What circumstances would be willing [sic] to report computer intrusions to law enforcement?" The answers from 236 respondents broke down as follows:

Anytime Detected	6.8%
Could Report Anonymously	30.2%
Only if everyone else reported	21.7%
Only if mandatory by law	37.4%
Other	3.9%

Law enforcement has tried hard to de-stigmatize computer crime reporting and that effort may finally be bearing fruit. Indeed, CSI reported that "the most striking result of the 1999 study is the dramatic increase in the number of respondents reporting serious incidents to law enforcement: 32% did so, a significant increase over the prior three years, in which only 17% called the authorities."

Of course, none of the above-mentioned business concerns explains the most common reason for failing to report computer attacks: most victims do not know they have been victimized. It has long been accepted as true that most computer crimes are not detected, but proving the extent of this problem -- that is, proving what victims do not know -- is obviously difficult. Fortunately for those attempting to quantify the problem, the Defense Department did a controlled study in which they attacked their own systems, thus providing accurate penetration and detection rates. Simply put, of 38,000 computer attacked, 24,700 (65%) were penetrated successfully. Only 988 (5%) of those penetrations were detected, and only 247 of the penetrated sites (27%) reported the intrusion. See generally, GAO Report on Computer Security, June 1996.

There are, however, prudent, cost-effective steps that companies can take to reduce their risks. These steps include mapping networks; marking critical information; developing internal policies and procedures relating to access controls, appropriate computer use, and encryption; educating users on computer issues, including social engineering; testing compliance with policies and procedures; installing firewalls, virtual private networks, and intrusion detection systems; and conducting attack and penetration testing. But doing security comprehensively does take resources and skilled personnel. Today, information resource dollars are more likely to be spent increasing efficiency, not security. And skilled personnel are hard to find as demand far exceeds supply.

Even if all companies were vigilant, there remain some difficult problems ahead which no government or business can solve alone. The first is jurisdiction. In the physical world, one cannot visit a place without some sense of geographical location. Whether a particular street address or continent, human travel is spatially based. By contrast, one can access a computer remotely without knowing where, geographically, that computer is located. Thus, even a small business can now be a global business, and may be subject to the law of any country whose citizens find the business's website. To the extent that nations have different consumer protection laws and criminal laws, the core question becomes: how do sovereign nations protect their citizens, and enforce their national laws, on a global Internet?

These international challenges are substantive, procedural, and technical. Substantively, many countries lack computer crime laws, which can make it difficult to obtain foreign assistance in an international case. This may serve to deprive small businesses of redress when they are victimized. Procedurally, slow international mechanisms for sharing critical investigative information may cause investigations to fail.

But such problems can be remedied, albeit not simply, by changing laws and procedures. Perhaps far more difficult are the technical challenges. Here, it must be remembered that the Internet does not provide for traceability, emboldening those who would commit transnational crimes. The fact that individuals can be anonymous or "self-identifying" (i.e., they can use

anonymous remailers and adopt false personas by providing inaccurate biographical information and misleading screen names) means that with increasing frequency those who abuse small businesses will not be identified.

There is, unfortunately, no simple solution to this problem. Building more reliable identification mechanisms into Internet protocols would require the efforts of internationally recognized, market-based, standards-making bodies whose agenda does not directly include public safety. Moreover, such mechanisms would be controversial, since there are strong reasons to allow anonymity in communications networks. For example, whistleblowers may wish to remain anonymous, as may a group of rape victims who wish to convene an electronic meeting to discuss their experiences without revealing their identities. Indeed, more traditional communications systems offer anonymous communications; calling from a pay phone or mailing an anonymous letter is a common practice, even if those techniques are sometimes abused.

But the difference between traditional means of communication and the Internet is significant, and attempting to solve Internet problems only by drawing analogies to existing technologies normally fails. For example, the telephone and mail systems allow for predominantly one-to-one communications. Although someone wishing to defame a public figure or harass women can call thousands of people anonymously, the time and cost make this impractical. By contrast, the cost-free, simple, one-to-many nature of the Internet alters the scope and impact of communications. It is this difference which explains why children who would never spend their weekly allowance buying "The Anarchist Cookbook" at a college bookstore will download the same information from the Internet and injure themselves testing a recipe. Because of the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the great debates in the years ahead.

The future will require that we tackle these problems, as future computer crimes may well be more sophisticated and disruptive than anything we have seen to date. The fact remains that many hard-core criminals, such as organized crime groups and terrorists, are members of a generation that came of age before computer technology, and they may not yet fully recognize how valuable computers can be in executing criminal schemes. Future generations will be computer literate, and the criminal element can be expected to use these tools extensively and successfully. As stated in one seminal report, "Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." Report by the National Research Council, an arm of the National Academy of Sciences (quoted in The Washington Times, December 24, 1990).

Indeed, as time passes, we continue to see more sophisticated and disconcerting conduct by hackers. The use of automated hacking tools allow even unsophisticated hackers to pose a serious threat to the security of systems. We have also seen more sophisticated attacks -- SYN flood attacks were replaced by the distributed denial of service attack -- which are very difficult to prevent because they exploit the current network architecture, or exploit flaws in the underlying protocols that allow computers to communicate in the first instance. Thus, computer security requires continued vigilance by technically literate personnel, a challenge for a small business with limited funding for computer security and an inability to find technically literate staff.

Chairman BOND. Mr. Charney, that is rather depressing.

We now turn to a man who may have some of the answers to begin the discussion. I have to apologize in advance, I have to be someplace at 10:15, but I will be back. The full statements of all of you will be submitted and included in the record. I will turn this over, when I leave, to Senator Burns.

Senator BURNS. I will turn it over to Paul Conlon.

Chairman BOND. OK. Paul and Damon will continue the discussion.

But now it is a real pleasure to introduce Roger Farnsworth, manager of product marketing of Cisco Systems in San Jose, California.

Mr. Farnsworth, welcome.

STATEMENT OF ROGER FARNSWORTH, MANAGER OF PRODUCT MARKETING, CISCO SYSTEMS INC., SAN JOSE, CALIFORNIA

Mr. FARNSWORTH. Thank you, Chairman Bond, Senator Burns, distinguished Members of the Committee and their guests. I want to thank you for the opportunity to come here today and speak with you. As a professional nerd, it is exhilarating to be able to put on a suit and rub shoulders with—

Chairman BOND. I was going to say what a nice looking suit that is.

Mr. FARNSWORTH. Thank you very much. My name is Roger Farnsworth. As you said, I am a manager of marketing for Cisco in the area of network security. As you may know, Cisco is the world's largest manufacturer of equipment that connects people and businesses to the Internet. We are also widely acknowledged as the leader, if not one of the leaders, in providing security solutions for the Internet economy. Cisco employs over 26,000 employees, headquartered in San Jose, California with major presences, as Senator Kerry said, in Massachusetts, North Carolina, and Texas.

Questions of security and Internet security are particular timely right now, especially with the recent incidents of denial of service attacks against high-visibility web sites. These issues are important not only to large companies but to companies of every size. The No. 1 reason people cite for not buying online today is fear for their privacy or the security of their transactions. Today I am here to suggest that these concerns can be addressed, security fears should not deter America's small businessmen and women from going online, and encourage all members of the industry to participate in finding the technological and operational answers to these problems.

A few years ago, Cisco Systems boldly predicted that the Internet would change the way we work, learn, live, and play. At that time these types of hacking incidents probably would not have raised the eyebrows and achieved the visibility that they are today. Today it is a different story. An attack against an online business or the digital domain has far-reaching ramifications and can be considered an attack against all of us because of the way the Internet has transformed our lives.

Some interesting statistics. Today nearly 40 percent of small businesses in the United States are now online, up from just 19

percent in 1998. Last year the Internet economy generated more than $500 billion in revenues and 2.3 million jobs in the United States according to a University of Texas study. Interestingly, of 3,400 businesses surveyed to measure the size of the Internet economy, more than one-third did not exist before 1996.

This expansion so far is astounding, yet the growth is likely to continue. Analysts estimate more than 3.5 million small businesses will be online next year and the Internet economy will be worth $2.8 trillion in 2003.

Business leaders recognize the strategic role the Internet plays in their company's ability to survive and compete in the new millennium. If you are a retailer and you did not have a yellow pages ad a few years ago, you were severely handicapped in your ability to perform your business. If you were a bank in the 1980s and you failed to add an ATM machine to your branch, you risked losing deposits of business. Today businesses should be looking into online banking, bill payment, or lending or face severe restrictions in their ability to grow their business.

Making money in the new millennium means facing up to the reality that you either go online or go home. This is particularly true for small and medium businesses, because frankly the competition from large operators has never been more fierce. The big dog is not just the chain operation across the street; in the Internet economy it can be a company you have never seen before because it is out of town, out of State, or out of country.

For some, that is going to be pretty frightening. But there is also a great opportunity here for small and medium business because everybody is the same size in the box sitting on your desk. The Internet levels the playing field between large and small businesses.

Amazon.com, for example, realized it could leverage the efficiencies of the Internet to take on the likes of Crown Books and Barnes & Noble. Online booksellers can charge just 5 percent gross margin while equaling the return on investment that brick-and-mortar booksellers can only achieve by charging 30 percent margins. Similar economies of scale can be applied to many small and medium business categories and we are starting to see companies taking advantage of that.

Smaller companies will continue to seek online opportunity. The key to competing in the Internet economy is recognizing the efficiencies of online commerce and moving faster than the other guy to take advantage of them. In the Internet economy, the big no longer beat the small. The fast defeat the slow. To accommodate the new model, the industry has worked very hard to build wider digital highways to carry more online traffic more quickly. Everyone agrees that faster access to the Web is a good thing. But as the recent hacker attacks show, a few misguided or challenged individuals can cause havoc by blocking these highways.

Unfortunately, you cannot always stop these people from doing their bad deeds. But you can work to more quickly recognize these incidents and deal with them. The Internet, by and large, is still a very safe place to be. It is an essential part of today's business. What we have seen in recent weeks was a pothole on the informa-

tion superhighway. Internet commerce did not stop. It slowed at a few sites for a limited amount of time.

Businesses do need to step up and improve their Internet security. Security is essential if a company is going to successfully compete in the Internet economy. If you have a business that is brick-and-mortar you generally have an alarm system and locks on your doors. If someone shakes the handle, hopefully your alarm contacts the police. You should use the same types of technologies to protect your online business.

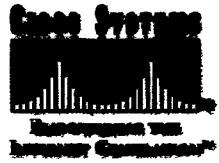
Our online consulting team has indicated that the types of incidents that have been reported here, tragically, very common. We recommend that small businesses take a risk-based approach to solving these problems. Use an array of products, including firewalls, authentication systems, intrusion detection systems, and vulnerability scanning tools to protect your business.

I brought today with me 10 tips for Internet security for small and medium businesses. These are by no means a comprehensive list of tips. These are probably the most common. I would encourage you to go online and look for information on Internet security. Cisco has a web site, www.cisco.com/go/security that can help you understand issues of information security and how you might use tools.

I will further say that as we heard a minute ago, the expertise in this area is rather centralized. The good news is that many service providers and consulting houses are now offering their expertise to small and medium business. In addition, companies such as Cisco and others are making available lower cost and usable tools for small business to use. For example, in the past year Cisco has bundled firewall software as well as intrusion detection software in some of our low-end routers to allow small businesses to deploy connectivity to the Internet in a cost-effective and safe manner.

Again, I want to thank you very, very much for the opportunity to speak with you today. Cisco is very interested in solving these problems and we feel that one of the most important ways to address these issues is through public forums such as this where we can come together and talk about methods that we can use to protect ourselves and each other.

[The prepared statement and attachment of Mr. Farnsworth follow:]



Hearing on Cyber Security for Small and Medium Businesses
Senate Committee on Small Business
Mar. 9, 2000

Testimony of Roger Farnsworth
Cisco Systems Inc.

Chairman Bond, Senator Kerry, distinguished Members of the Senate Small Business Committee, I appreciate the opportunity to speak with you today about security on the Internet for small and medium businesses. My name is Roger Farnsworth and I am a manager for security products marketing with Cisco Systems Inc. As you may know, Cisco is the world's largest manufacturer of equipment that connects people and businesses to the Internet. It is also a leading provider of security systems and expertise. Cisco employs 26,000 people, is headquartered in San Jose, California, and also has significant operations in Massachusetts, North Carolina and Texas.

Questions of security are particularly timely right now, as you know, in light of the recent wave of distributed denial of service attacks against big-name Web sites such as CNN.Com, EBay, E*Trade and Yahoo! And these issues are important to companies of every size as they begin to realize the power and value of e-commerce. The No. 1 reason people cite for not buying on-line is fear over security or privacy. Today I'm here to suggest that these concerns can be addressed, and that security fears should not deter America's small businessmen and women from going online.

A few years ago, when Cisco Systems boldly predicted that the Internet would change the way we work, live, play and learn, hacking incidents of this type might have been mildly interesting but certainly wouldn't have been cause for alarm. Today, it's a different story. An attack against the digital domain can be considered an attack on us all because the Internet has become such a driving force behind the new global economy.

- Nearly 40% of small businesses in the United States are now online, up from 19% in 1998.
- Last year, the Internet Economy generated more than $500 billion in revenues and 2.3 million jobs in the United States, according to a University of Texas study.
- Of 3,400 businesses surveyed to measure the size of the Internet Economy, more than a third did not exist before 1996.

This expansion so far is astounding, yet the growth is likely to continue. Analysts estimate more than 3.5 million small businesses will be online by next year, and the Internet Economy will be worth $2.8 trillion by 2003.

Business leaders recognize the strategic role the Internet plays in their company's ability to survive and compete in the new millennium. If you're a retailer, you went out of business a few years ago if you didn't have an ad in the yellow pages. Now, you've got to have a Web site or you lose a large portion of your potential shoppers. If you were a bank in the 1980s, you had to add an ATM machine

outside your branch or risk losing deposits. Today, you'd better be looking into online banking, bill payment and lending or your competitors will do it first and put you out of businesses.

Making money in the new millennium means facing up to the reality that you either go online or go home. This is particularly true for small and medium businesses because, frankly, the competition from large operators has never been more fierce. The big dog isn't just the chain operation across the street; in the Internet Economy it can be a company you've never seen because it's out of town, out of state, or out of the country.

For some, that's going to be pretty frightening. But there's also a great opportunity here for small and medium businesses because everyone is the same size in that box sitting on customer desktops. The Internet levels the playing field between large and small businesses. Amazon.com, for example, realized it could leverage the efficiencies of the Internet to take on the likes of Crown Books and Barnes & Noble. Online booksellers can charge just 5% gross margin while equaling the return on investment capital that brick-and-mortar booksellers can only achieve by charging 30% margins. Similar economies of scale can be applied to many small and medium business categories and we're starting to see many companies taking advantage of that. Smaller companies will continue to seek online opportunities to increase their visibility and compete with larger establishments.

The key to competing in the Internet Economy is in recognizing the efficiencies of online commerce and moving faster than the other guy to take advantage of them. Time becomes the great differentiator rather than size. The big no longer beat the small. In the Internet Century, the fast defeat the slow.

To accommodate this new model, we as an industry have worked very hard to build wider digital highways to carry more online traffic more quickly. Everyone agrees that faster access to the Web is a good thing. But, as we saw with the recent hacker attacks, that's a double-edged sword. By continually improving this efficient highway system, we make it possible for a few misguided or malicious individuals to block traffic on the highway for everyone else. Unfortunately, you can't always stop people from running into the middle of the road to cause a problem. The key is how quickly you detect, respond and clear the traffic jam.

The Internet is still by-and-large a very safe place to be. It's still an essential part of today's business. What we've seen in recent weeks was a pothole on the information superhighway. Potholes happen. But Internet commerce didn't stop, and it won't stop any more than you'd expect a restaurant to shut its door after a break-in or a power company to shut down after a storm-caused outage.

However, businesses do need to step up to improve their Internet security and awareness. Security is essential if a company is going to successfully compete in the Internet Economy. Whether you're a small, medium or large business, you have to take a holistic approach to securing a network. At home, you leave a light on at night to deter burglars. You lock your doors and windows. You might have an alarm system, and when triggered that alarm might call the local police department. Network security deserves the same attention – no more, no less – that you give to your brick-and-mortar business.

Cisco has a well-respected security consulting team that has evaluated the security posture of hundreds of networks over the past few years. Based upon our extensive evaluations of the strengths and vulnerabilities in all types of systems, we acknowledge that no network can ever be 100% secure. However, companies that are serious users of the Internet should take a proactive approach to Internet security with the goal of developing an intelligent self-defending network that eliminates

most risks. This would be a systems approach to security where an array of products work together to recognize threats, implement policy in a distributed fashion and enforce security in a consistent manner, dynamically and in real-time.

A number of technologies and services are increasingly important to Internet security. These include the ability to provide identity infrastructure, perimeter security, data privacy, security monitoring tools and policy management. Cisco believes that, in the future, these types of solutions will become increasingly integrated in the fabric of customer networks. They will be ubiquitous, appearing at all access points and all places in the network where information moves. Most importantly, we believe these tools will be transparent to the end users -- the customers. This is critical because users have a strong aversion to roadblocks that make it more difficult to get where they're going on the Internet, things like password windows, grant/deny authorizations and so on. By implementing a transparent, ubiquitous and integrated security solution -- or an "intelligent self defending network" -- small and medium businesses can enable customers to reap the benefits of the Internet Economy.

Now many small and medium businesses don't want to deal directly with any or all of these issues. They cannot afford complex defensive systems or teams of security professionals. And the good news is, they won't need them. More than half of small businesses will outsource responsibility for running their corporate Web sites to an Internet Service Provider or Web Hosting company. The ISP or Web Host will be tasked with securing the sites. And smaller sites with fewer points of contact to the network are generally less likely to face the same attacks that high profile sites invite.

Nevertheless, small and medium businesses can take some basic online precautions to protect themselves, their employees and their customers that do not increase costs or require full-time experts. Included with my printed testimony are a preliminary list of 10 Basic Cyber Security Tips for Small and Medium businesses. These are also available on Cisco's public Web Site at www.cisco.com/go/gov, under Net News.

I hope that my comments today have been helpful to you and your constituents. Again, thank you for having me here. I'd now be happy to walk through our ten cyber tips or entertain any questions you may have.

CISCO SYSTEMS' "10 BASIC CYBER SECURITY TIPS FOR SMALL BUSINESSES"

1. **Encourage or require employees to choose strong passwords.** Hacker programs available on the Internet contain tens of thousands of common passwords, which can be used to break into unsecured computer systems. A password should have a minimum of 8 characters. They should be non-dictionary words. They should combine upper and lower case characters. You can even mix in a symbol, like a $. An ideal password might be something like 2B3#N3$.

2. **Require new passwords every 90 days.** By the time a hacker gets your password, it will already be outdated.

3. **Make sure your virus protection subscription is current.** Most businesses purchase virus protection programs from companies like Norton or McAfee. These companies regularly offer patches and updates to their programs to respond to new threats. Companies should regularly check for defense improvements and be sure their subscription to virus protection updates remains current.

4. **Educate employees about attachments.** Just because it's in the "in-box" doesn't mean it's been cleared through any security mechanism. Attachments, particularly executables (with .exe at the end) can be dangerous, dropping off a little software code called a "Trojan Horse" that corrupts your system or allows it to be infiltrated at a later time. Employees should be educated about security basics, including the need to avoid opening attachments from unknown sources.

5. **Install a total solution.** If you're securing your own system (instead of relying upon an ISP or web host), don't just throw a firewall at a network and call it secure. Firewalls do a great job of securing a perimeter, but no one device will do the trick. Complete solutions should include firewalling, intrusion detection and policy management.

6. **Assess your security posture regularly.** Don't secure and run. Hackers are constantly updating their technology. Small and medium businesses need to know how they stack up against the most current types of attack. If you're relying on a Web host or ISP, be sure to choose a vendor who is security savvy. Compare their offerings to those of other companies.

7. **When an employee leaves a company, remove the employee's network access immediately.** When asked to evaluate the internal security posture of networks, the Cisco Security Consulting team finds vulnerabilities in almost every network tested. Just as you ask departing employees to turn in their keys to the front door, you should take away their key to the network when they leave. Disgruntled employees are the greatest threat to any systems' security.

8. **If you allow people to work at home, provide a secure, centrally managed server for remote traffic.** Telecommuting increases worker satisfaction and productivity. But it also presents a security challenge. It makes little sense to spend $10,000 on a security system for your Web site while you allow people to dial-in to your network unabated.

9. **Update your Web server software regularly.** Stay on top of security updates and patches. These are often available for free over the Web. Make sure you're always running the latest versions of software to stay ahead of hackers, who are certainly working to stay ahead of you.

10. **Don't run any unnecessary network services.** If your employees don't need Web access, don't provide it. If you don't need services such as NFS, Finger, Echo or some of the other programs that are routinely provided with software suites, make sure they're turned off. Often, a variety of services are provided by default in a program. Exploitation of these services is one of the most common hacks seen by Cisco's customers.

Senator BURNS. Thank you very much, Mr. Farnsworth. Sitting here listening to your testimony, and interested in business—whenever the denial of service thing happened with those major businesses, business did not stop. But I think it sent a chilling warning through the community of people who use services on the Internet. I think what you brought along today points out that—they will probably be taken more serious now than they would have say just a month ago.

Education and awareness is probably our biggest challenge right now as people try to protect themselves and try to protect their web sites.

Yesterday I asked, is there a technology, in the area of denial of service that really jams it up, is there a technology that serves like a thermostat when you are nudging up to a point where your load is such that it allows you to take some actions that may prevent something like the denial of service?

Mr. FARNSWORTH. Yes, Senator Burns, one of the things that we encourage—

Senator BURNS. I realize this one happened all at once. I mean, just instant.

Mr. FARNSWORTH. Let me point out two things. When the first incidents of these types of denial of service attacks occurred back in the fall of last year it took approximately 3½ days for the leading consultant teams to determine the source of the attacks and put them down. The most recent incidents are being detected and responded to and solved in a matter of hours, if not minutes. So our skill at detecting these types of attacks is improving.

The other question you raised about a type of thermostat is a good question. Cisco has been encouraging our large service provider customers as well as our large enterprise customers to implement some tools. There is a particular tool called rate limiting, for example, that can be placed on certain interfaces of the Internet backbone routers which can, in fact, set thresholds for this type of traffic. And if those thresholds are approached or exceeded, this type of traffic can be throttled before it becomes a significant problem to an end system.

The issue there is that this is an issue that everyone has to address because it has to be implemented at all areas of the network in order to become effective. That is why we are encouraging all members of business to take a look at their procedures and see if they are addressing this.

Senator BURNS. Now another question I did not get to yesterday—by the way, we had a terrific hearing yesterday. Now we know that what happened to eBay in this denial of services, and Yahoo, was the enlistment of, or the use of computers dropping—you know, in other words, very successfully entering somebody else's computer, setting a program in there that can be triggered by me, and those computers can be found all over the United States. I think they finally found some of them located in some learning institutions, were found that way.

Tell me about how do I protect my computer, my system on my web site from being—from one of these—I guess you could not call

it a cookie really—but a program to be imbedded in there and to be used by somebody else without my knowledge?

Mr. FARNSWORTH. That is interesting. We would call that a malicious applet or malicious code being placed on your computer.

Senator BURNS. I tell you what, we got to learn a whole new vocabulary. Got to get out a new dictionary here.

Mr. FARNSWORTH. Your point about educational facilities being a primary target is well taken. Historically, those were the most publicly available sites that were online 100 percent of the time.

What is very frightening to us now is the emergence of a new type of online access for the private home user, digital subscriber line service, or DSL service, or cable modem access. These types of service mean that home computers that are turned on and connected to the Internet become accessible to the Internet 24 hours a day. So it is not just the Government and educational facilities that we have to worry about now.

Using virus scanning programs that are able to detect these types of malicious applets is something that people should do religiously. Not just the educational and Government facilities, but every user of a home computer that connects to the Internet. Recognize that if traffic can go out from your computer to the Internet, it can come in. So make sure that you look at your PC or your computing work station and take advantage of the advances that virus scanning companies are making; companies like McAfee and others. They do a very good job of detecting and reacting to the most recent virus profiles and malicious code profiles. And you need to be aware of that and use these programs as a normal part of—

Senator BURNS. Are you saying then, let us say my computer at home. When I leave I should turn it off?

Mr. FARNSWORTH. Yes, sir.

Senator BURNS. When it is off, is it accessible to outside entry?

Mr. FARNSWORTH. Generally speaking, no, sir. Generally speaking, once you turn your PC off and there is no longer power applied to it, it is not accessible. There are certain exceptions to that with systems that are what we would say, Energy Star compliant, that can——

Senator BURNS. Can be turned on?

Mr. FARNSWORTH [continuing]. Recognize stimulus and wake up. But generally speaking, home computers are not vulnerable to that type of attack.

Senator BURNS. In other words, when I am not home, turn the damn thing off?

Mr. FARNSWORTH. That is a very good idea.

Senator BURNS. I will tell you, you know, our kids had to teach us how to use these computers. Now you got to remember—because us old ducks, you know, they were strange and we were afraid when we first started fiddling around with them that if you hit wrong key, the thing would blow up. But we later found out that computers are kind of like mules. You cannot make them do what they do not want to do. And you have got to be smarter than the mule, and I am having a hard time with that, as you well know.

[Laughter.]

Senator BURNS. I have got to leave and I understand you are going to form a dialogue here now with these folks here. But I

want to—I appreciate you coming today. We did talk about—Ms. Riley, I am going to also ask you, if the Secret Service is into the enforcement of some laws and then we also have the center, we are building a center for the FBI so they can deal with these things, have we done an overlap of law enforcement agencies that are starting to deal with crimes regarding the Internet?

Ms. RILEY. That is an excellent question, Senator. I think one of the most important things to note there is that there is a concerted effort on the part of all law enforcement, whether it is State, local, or Federal, associated with CyberCrime to share information on a regular basis. To ensure that if we are working an investigation involving a target that has hacked into four businesses, that we are sharing that information and sharing investigative leads early on. So that if another agency is working an investigation into that particular target, that we are sharing the information very quickly.

The issue is that CyberCrime is not defined only by hacking activity. The specialized skills that we have, for example, in the financial networks or in the telecommunications networks used to be some very traditional offenses involving things like credit card fraud and bank fraud. A lot of those traditional offenses have now migrated onto the Internet. That does not change the fact that the expertise we have in those financial investigations is not there with our investigators any more. We just have to add skill sets to those investigators to work them in the Internet environment and in the cyber-arena.

I think every agency that has traditional offenses, whether it is child pornography with Customs, or weapons trafficking with ATF, all of those agencies have a very core expertise in working those types of cases, and it brings a lot of value into our enforcement efforts between all the very different agencies. But the key is that we are sharing information between agencies.

Senator BURNS. Do we have a central point where we are collecting the information, or one particular agency that is in charge of that information and building databases of cases?

Ms. RILEY. On all types of CyberCrime?

Senator BURNS. Yes.

Ms. RILEY. No, not one central database. We do—

Senator BURNS. We got to talking yesterday about—you know, I am going to bring an old culture forward a little bit. Some way or other we have got to put a warning on these—some of these hackers and people who cause mischief on the Internet are young folks who are just kind of searching and just playing games. Some way or other we have got to warn those people that they are venturing into an area where they could be prosecuted under Federal law.

I can remember as a child the first thing you learned, even though we had open mailboxes, we did not fiddle around with somebody else's mail. There was a warning there that said, Government property and if you touched somebody else's mail, why you could go to jail. I am wondering if we should not do that with some technology or something that says, you are wandering into an area where you could be prosecuted?

Yes, Mr. Charney?

Mr. CHARNEY. Yes, I would like to address that point, because first of all many computer systems do have banners warning them.

But more importantly, it is an ethics and education problem. The Justice Department with the Information Technology Association of America has announced a cybercitizen partnership which is funded by the Justice Department and industry and it is an ethical campaign for children, to teach children the ethical use of computers.

Senator BURNS. I think that is notable, because awareness on this type of thing is very, very important.

Ms. NEPTUNE. I would also like to make a point on that, because this all goes back to the parents. I think that one of the problems with the Internet is that it is not regulated, and it is not a per-minute service. It started out free. It is not regulated, but it is a telecommunication service just like regular long distance.

If it was regulated by the FCC, although there are problems there with small business, but if it was regulated by the FCC and the telephone companies charged per-minute rates, the Internet service providers would have to pass that along to the consumer. And when the parents got their bills I think we would have a lot of control over the children just like we have had elsewhere. I know that is not a very happy thought.

Senator BURNS. I think she has thrown out quite a lot of fresh meat here and you guys will have quite a lot to talk about.

Ms. NEPTUNE. I know you Internet users do not like to think that way but I do believe that that time will come because the Internet service providers cannot make a profit anyway if somebody stays on—

Senator BURNS. I have got another appointment here and I am going to go take care of that. I am going to throw that out and leave it for your discussion. I am going to leave it to these gentlemen here, and they will know how to handle all this.

Thank you for coming and participating in this and for your time. We know that you have got other things to do. We happen to think that this is very, very important to small business, the Small Business Committee, and over on Commerce as far as science, technology and communications is concerned. Just like I say, with the Justice Department yesterday I asked the gentleman then, has he had any communications with Congress and how do they want Congress to react to these type things? Should we be looking at a different approach and how can we partner on trying to prevent what happened to Ms. Neptune and also this denial of service shutdown.

We keep the lines of communication open. We have just got to do that because we know that we are dealing with an entirely different kind of situation that we have never dealt with before. And everyone of us are sort of dumb about this.

So again I want to thank you for coming, and Paul and Damon thank you for inviting them.

Mr. CONLON. Let me do a little bit of housekeeping first. Before we go around and introduce all our participants, if there are any participants in the audience that have not come up and taken their seats, it is an opportunity now to come up. Would you like to go ahead and introduce yourself, Mr. Keam?

Mr. KEAM. Sure. My name is Mark Keam. I am assistant chief counsel with the Office of Advocacy at the Small Business Administration.

Mr. GLOVER. Jere Glover, chief counsel for Advocacy.

Mr. DUGGAN. Marty Duggan, Small Business Exporters Association.

Mr. DEBOW. Charles DeBow, National Black Chamber of Commerce.

Mr. BARTON. Richard Barton with the Direct Marking Association and also the Association for Interactive Media and the Internet Alliance which is part of our group.

Ms. BAHRET. Mary Ellen Bahret with the National Federal of Independent Business.

Mr. DOZIER. Damon Dozier, Senate Small Business Committee minority staff.

Mr. CONLON. Paul Conlon, Senate Small Business Committee.

Abe Schneier. Abe Schneier representing the National Alliance of Sales Representatives Associations.

Ms. RIVERA. I am Maritza Rivera with the U.S. Hispanic Chamber of Commerce.

Mr. PAGE. Matthew Page with the Small Business Legislative Council.

Mr. MORRISON. James Morrison with the National Association for the Self-Employed.

Mr. LANE. Rick Lane with the U.S. Chamber of Commerce.

Ms. JACQUES. Veronica Jacques with the Direct Selling Association.

Mr. CONLON. Before I open the discussion I just want to ask one quick question to Ms. Neptune. What advice would you give to another small business given the experience that you have had?

Ms. NEPTUNE. It is very difficult to say but Mr. Charney's remarks were right on key. I mean, every point that he made is a problem for small business. We were unique because we were an Internet service provider so our concerns would be different than a small business who is doing e-commerce over the net.

I do believe that you have to get a very good systems administrator, and there are problems finding that. You have to invest in some firewall software, virus detection that automatically comes up on your computer every morning. It is not going to catch everything, but it does help. Changing your passwords and make sure your systems are behind firewalls and you turn those systems off. It is not going to protect you all of the time.

He also made a very good point, technology changes every day and small business does not have the money to go out and do that. We can only do as much as we can.

I would also say that small businesses should join trade associations where they can pool their resources and share the information.

Mr. DOZIER. I think it is probably appropriate at this point if a member of the forum here would like to be recognized, it is probably best if you turn your card up so that we can acknowledge you, and then we will try to get everyone's comments in turn.

I think one of the comments that got the most head-shaking was the comment about regulation of the Internet which seems to be a very, very controversial issue. I think Mr. Lane wanted to say something about that, with Paul's permission.

Mr. CONLON. Go ahead.

Mr. LANE. Probably one of the most stifling aspects of the EU (European Union) is that they do charge a per minute charge for the Internet and it does stifle innovation and its use. We have seen it grow. So we would not support a permanent charge for the Internet, nor certain regulations of e-commerce.

I am the co-chair for the policy committee for the Partnership for Critical Infrastructure Protection, and we are looking at a lot of the policy issues. Partnership for Critical Infrastructure Protection is a group of about over 120 corporations that are working together, trying to figure out a lot of the issues that we are discussing today.

But some of the general consensus is that the Government should not mandate the level of security. Security changes too quickly. You just cannot keep up and say here is the standard, because as we know, security is a process and it is constantly changing and there is a cost associated with constantly trying to update to standards that are constantly changing.

The marketplace does a pretty good job of doing that, such as web-hosting facilities where small businesses can sell or use a web-hosting facility to help protect their Internet.

One of the things that small businesses and the Government should be working on is a sharing of information. We should look at FOIA (Freedom of Information Act), so businesses can share information with one another. We should also look at increasing punishments for those who are hacking.

We should make sure that we are not putting liabilities on small businesses, because they already face liabilities. I think Ms. Neptune hit the nail right on the head. Her cost of her business, it was just decimated. So to add on top of that, additional liability to small businesses when they do get broken into would just be ridiculous, because they already pay a heavy, heavy price as we see things moving forward.

Security is a process and we need to ensure that we are educating our employees. Most of the trouble does not come from the outside; most of the trouble comes from employees from within who are stealing that information.

One of the other things that we need to look at that is being discussed a lot here in Washington, is access to personal information. The problem with that is if you allow easy access to my information on a web site, that means you make it easier for everybody else to access that information. So we need to be very careful when we are talking about access, and you hear about that a lot, that we think we are not, in fact, compromising security, when actually we are.

Mr. CONLON. Would anyone else like to add something to that? Mr. Duggan?

Mr. DUGGAN. I think that the things that you talked about were all preventive type things that corporations could do, and I think that that is each corporation's responsibility. They should have due diligence in everything that they are doing.

I think that from the standpoint of the hackers, the people who are abusing the system and taking advantage of the system, is that I would think there needs to be, if there is not already, Federal legislation where you have got uniform or mandatory sentences where people know that there is a price to pay—that they cannot go in there and wreak havoc on somebody's business, and to the cost to

a small company of a half a million dollars, and for others maybe in the billions by the time they get through, that there is going to be one hell of a price to pay.

I think the deterrence has to be part of the education which was mentioned earlier. You let hackers know that there is going to be one big price that they are going to have to pay for doing what they do.

Mr. CHARNEY. Can I respond to that comment? The U.S. Sentencing Guidelines do, of course, have penalties for computer crime. And if you are convicted under 18 USC 1030(a)4, the fraud provisions, or (a)5, the damage provisions, there is a mandatory sentence.

The difficulty is twofold. First, in the case that we heard about, the defendant was not in the United States. A country may not extradite their own nationals and you cannot impose U.S. law on foreign countries. So the international cases are tough.

Second, the real deterrence is more the certainty of getting caught rather than the actual sentence you will receive. Because defendants do not sit back and say, "I think I will do this because I will only get 3 months as opposed to 6." What they worry about is, "Am I going to get caught in the first instance?"

If you look at the clearance rate for computer crimes, that is the number of computer crimes solved in the hacker environment, it is incredibly low. Homicides run from 70 to 90 percent. Hacker cases are very, very low.

The reasons for that are many, but the bottom line is the Internet allows for a large degree of anonymity, global reach, and there is no traceability. When someone is victimized, you now need evidence to find the source?

In the United States, due to market forces and privacy concerns, providers do not keep data. In Europe, you have the European data directives and telecom directives, and they are not allowed to keep data. Which means there is no way to do a historical investigation and there is no way to catch anybody.

So if you really want to look at the fundamental problem, about why people are not deterred, you have to look at the clearance rates and ask, "Why is the Government not finding more people?" That is not a criticism of the Government, because I was there up until 4 months ago and did this for 9 years. The technology does not support finding people.

For some reasons that is good, if you are exercising first amendment rights and shopping, that is fine. But bad guys are not held accountable. That is a problem and it is going to be here for a while because of the competing interests. You just cannot have traceability on the Internet. It raises too many technical concerns, Government mandate concerns, and privacy concerns.

Mr. LANE. There is also the Digital Millennium Copyright Act that is out there, as well, which makes it both a civil and criminal crime to circumvent what is known as a copy control technology. So if you bypass somebody's password to get at copyrighted information—which you can argue most information is except for factual data—you can go after them both for civil and criminal penalties.

We want to make sure that "yes," there is no traceability, but we do not want to trample on civil liberties, because there is a fear fac-

tor out there. We need to make sure that we have a very balanced approach, so that way those individuals who do want to be anonymous, if you think about China, for example, where they are not anonymous and they can go after them, I do not think we want to have that type of oversight here in the United States.

At the same time, I do not know what the answer is. I am not going to come up with a solution, but it is a very difficult balancing act and we just have to make sure we are not trampling on civil liberties here, as well.

Mr. DUGGAN. I think what Mr. Charney said about the number of prosecutions, I think last year there were six. Certainly the abuse is a hell of a lot higher than that.

Mr. CHARNEY. Believe me, the Government has been throwing a lot of resources at this. I mean, Ms. Riley can talk about what the Secret Service has been doing, the growth at the FBI, the 10 National squads and NIPC agents in every office. It is a fundamental problem.

Ms. RILEY. I would like to point out too though, that the statistics may not exactly mirror the efforts on the part of law enforcement in prosecution. For example, in the investigation involving Ms. Neptune's company, that was centered around credit card fraud. So when you pull a hard statistic from the national criminal information databases, it is going to reflect a credit card fraud investigation rather than a hacking investigation.

So a lot of times where the Internet was used and was certainly a tool of the criminal activity, the actual offense that is listed in all of these statistics that are commonly cited, may certainly be reflective of the actual hacking activity but another type of crime.

We actually have gotten better sentencing, had this been in the United States for example, as was mentioned, this person was prosecuted in Germany. The good news is they did have computer crime laws that were applicable to the activity. That is not true in all countries. There are certain areas of the world where it is not a crime to do what they had done to Ms. Neptune's company.

But the United States, many times in consultation with the prosecutors—we used to have these conversations with Mr. Charney on a regular basis—the question was how can we get the best sentencing? How can we most effectively prosecute this case? And which statute, whether it is hacking or another type of criminal activity or another criminal violation, best applies to the activity that is here.

So I hate to hinge all of our prosecution investigative efforts in law enforcement based on statistics from only the computer crime statutes, because there are a lot of other violations that are charged that are really related to that activity.

Mr. LANE. Remember, Al Capone was charged on tax evasion.

Mr. CONLON. Mr. Glover.

Mr. GLOVER. There are a couple of things that are fairly exciting about this. No. 1, it is an industry made almost entirely of small business alumni, 10 years ago everybody in this industry was small business. It is really interesting. We just did a study that 76 percent of all of the jobs created in the whole information industry area are still small business, so it is still a small business industry.

But let me focus specifically on an area of fraud and crime that I think is going to become much more prevalent. We all know what is referred to as the toner cartridge scams that exist, where people call up and sell office supplies at multiple times what they were worth.

There is going to be a whole other assault on truly the small business users, and that is going to be real interesting because they are huge problems that we are all dealing with. There is another level of crimes that are going to be out there, and that will shake the foundation of a lot of people who start getting burned by buying and finding out that the funds they send through the Internet get flipped four or five times and may well end up internationally somewhere they cannot follow them. So there is a much lower level of crime affecting individual purchasers one at a time.

We spend a good bit of our time and resources in working with the SEC (Securities and Exchange Commission) and the FCC (Federal Communications Commission) and other agencies looking at making sure the general system works. But investor fraud, there are a whole bunch of areas where I think you are going to see a lot of things popping up very quickly. What I am afraid of is that the Government is going to be behind the learning curve and we are not going to react to these kinds of problems quickly enough, and we will see thousands of small businesses get burned on a one-on-one basis.

Mr. CONLON. Ms. Riley, maybe you want to follow up a little bit on that, in relation to what law enforcement in the United States is doing to reach out to law enforcement in other countries?

Ms. RILEY. Sure. There are several initiatives underway involving United States law enforcement with our international counterparts to address the high-tech crime issues and the traceability options that we have, in working these investigations across borders. There are a great number of restrictions that we are faced with in trying to work internationally. And that works both ways.

International law enforcement has those same restrictions in trying to trace criminal activity into the United States.

What is happening in one form, for example, the G–8 countries have a high-tech subcommittee that has been dedicated to working through options for law enforcement to be able to follow investigative leads, investigative traffic across borders quickly. Our biggest problem in high-tech law enforcement is that the records that we need to successfully investigate a case are only there and available to us for a limited amount of time. So speed is definitely of the essence.

Some of the work that is being done in this international forum is really geared toward expediting the political issues and the legislative judicial issues, in working through the international concerns that are there, and being able to work these cases through.

Now I have to say one of the most effective things that we have had though, and was especially true in the case involving Ms. Neptune's company, was that we had agents already stationed in foreign countries. They already had a relationship established with the local law enforcement.

So it was a case, in that particular instance, the German officials were able to open an investigation because of criminal activity that

did occur in Germany and work through the case very, very quickly. The relationships that we had already established worked very much the same way if we were to go into another city within the United States and work with another law enforcement agency.

So those partnerships were really key and we, as well as many other law enforcement agencies, intend to continue building those partnerships to be effective and quick at dealing with these types of investigations.

From the time Ms. Neptune called us to the time the German student was identified was only about 9 days. That is how quick all of this worked through. And it had to work that fast, or we would not have had the records to trace.

Ms. NEPTUNE. It seemed a lot longer to me, Mary.

But I would like to ask one question, now that I hear a lot of the concerns. Thinking back, I am very surprised, like what would I have done if it was not credit card and my corporate attorney—and I could afford a high-priced corporate attorney, some small businesses cannot—what would I have done? Because I would have had the threat, even if I sent the $30,000, I would have had the threat of this gentleman always coming back for more and more money.

So what would another small business do in that instance? Even now, where do they go? Local law enforcement?

Mr. LANE. That is one of the biggest problems. The Critical Partnership is looking at that, because when you get robbed in a small business you always go to your local police. And then if it is credit card fraud or something, you may go to the State level and then finally to the Federal level.

It is a similar type of process that you do go through. But for you, you were in 1996, so the computer security bill that we were just talking about was not enacted until I think 1998. And so now you can go to the Federal FBI and others, to have them come and try to take a look at this.

Ms. NEPTUNE. But would small business know that? It is very intimidating to say I think I will call up the FBI.

Mr. LANE. That is one of the things that the United States Chamber is doing. We are actually holding a network security conference on March 23 to talk about network security, where we will be web casting it, having our local chambers tying into that.

There is a whole host of education. The Small Business Administration is having small business week during, what is the week of that?

Mr. GLOVER. May 24.

Mr. LANE. So part of their effort is to educate. So education of small businesses, as Senator Burns was talking about when we were talking about DSL and cable modems, most individuals—and my brother is one—did not realize the threat that he has a cable modem, and the impact.

When I called him and said you realize all your financial information that is on that computer when you are doing taxes and Intuit and all the other fun stuff is compromised. And he did not know that.

So it is part of a massive education that we could partner with the Government, with the Small Business Administration, and

other groups around this table to be in a massive education effort, just as we are trying to do on the privacy issue, as well.

Ms. NEPTUNE. I do have one other question for the Small Business Administration. Is there a possibility that, just as you offered special loans for equipment that was necessary for Y2K, which nobody knew about when I called the SBA I might add, is there a possibility that you could offer some guidance and some loans for people, with some guidance on what they need to purchase for better security systems?

Mr. GLOVER. One of the interesting things when we talk to bankers, and we do most of our lending through bankers, we find that financing businesses in the information technology area is new for bankers and it is certainly new for everybody in the Small Business Administration. Historically, our lending patterns were based on brick-and-mortar and we are trying very hard to change that.

The Congress gave us special authority in Y2K to make those kinds of loans. I think it has done some good, to make sure that we learn a lot more about the people who need the money the most to grow in the new technology. But there still is a significant amount of resistance in banks about lending to information technology companies. They simply, all too often, are forced to go get venture capital or fail because nobody else understands the industry.

Ms. NEPTUNE. Because they want you to be in business 2 years and be profitable for a year. So it is very difficult to go to banking.

Mr. GLOVER. The life cycle of an awful lot of technologies today is so short that by the time you meet traditional standards it is too late.

Mr. CONLON. Can I just throw the previous issue back to Mr. Charney and Ms. Riley? Who does small business call?

Mr. CHARNEY. I want to go back to the issue of division of resources between Federal, State and local because it raises some very serious issues. Originally, the Federal Government got involved in CyberCrime in a big way because there were a couple of incidents, like getting hacked by the KGB, which required the Government to mobilize and become quickly knowledgeable. Because so many cases were interstate or international in nature, the Federal Government had a huge role to play.

But as the technology has simply exploded and you have more and more of this criminal activity, there is an increasing burden because the Federal Government cannot do it all. So the State and locals have to pull up and do some of this stuff.

There are programs underway, like the National CyberCrime Training Partnership which is a DOJ/State/local venture, to train State and local law enforcement. The difficulty is in large cities where they can dedicate some people to computer crime work, like New York and Los Angeles. In smaller towns it is much, much harder to do that because the resources are not there.

The difficulty is not just the amount of expertise needed to do these cases, which requires a lot of training, but also the budget implications of developing a CyberCrime unit in practice. I was a local prosecutor in Bronx County for 7 years in New York City. And when police officers came out of the police academy, they were given a gun, a memo pad, and a flashlight. Twenty years later they

turn those three things in, they still had them. They change bullets and paper and batteries, and that was it.

Now you go to the CyberCrime area and you go into a town, because we do a lot of roving training, and we go out and say "OK, you are going to need to buy all of this computer equipment and all of this training so you can do CyberCrimes". And they look at that as a percentage of your law enforcement budget and they panic. Then you hit them with the best thing, which is 2 years from now you are going to have to buy it all again, because it is all obsolete and you have got to start over.

The way the budgeting for this matter works has made it difficult for the Federal Government to keep up. The burden on State and locals is phenomenal in law enforcement, and the Congress is really going to have to rethink how to fund State and local initiatives on CyberCrime.

If you do not do that, they are not going to have the resources, it is not going to happen. The burden is going to fall completely on the Feds, the Feds are not going to be able to do all the cases that come in the door, and the system is going to collapse.

Mr. CONLON. Ms. Riley, if I am a small business and I have been the victim of some form of computer crime, I am not certain exactly what the details are, who do I call? What do I do?

Ms. RILEY. There are a couple of issues there. First of all, Mr. Charney is absolutely right. There is no way the Federal law enforcement can take every case that is out there. But in that vein, it is also incumbent upon us, with the experience that we have been able to build up over the last 15 years of working these cases, to train our local law enforcement counterparts to be able to respond to some of these investigations, as well.

To answer your question quickly, though, if you were the victim of a crime like this, call your State, local or Federal law enforcement agency. Picking up the phone and calling cold is OK, too. We get calls like that on a routine basis. If it is not the right place to call, if you have not called the right agency, who has the right expertise for your type of investigation, we make common referrals.

In fact, what is very common for us, if we know that a particular case does not meet a prosecutive threshold—and that happens and especially in some of the larger cities—if the case does not have a certain degree of loss associated with it or there is another prosecutive threshold that we are unable to meet on the Federal side, we do not want the case just to go away and the person to get away with it because of these thresholds. We will call our local counterparts and either work a joint investigation with them if they need our expertise or work with them through the investigation until they are comfortable taking that over.

There are some phenomenal CyberCrime units within a lot of State and local police departments. They are intent on increasing their technology and increasing their ability in these CyberCrimes. One example of an initiative like this was conducted between our agency and the International Association of Chiefs of Police.

They were concerned that State and local law enforcement at every level did not have the expertise to be able to appropriately seize computer evidence, whether they saw it in a traffic stop or they ran into it in connection with a homicide investigation or some

other non-traditional CyberCrime, they did not want them ignoring that evidence, that was very important, just because of a lack of training.

They requested that we work together in an initiative to put a quick guide together that could be distributed to all law enforcement; it was written at a level all law enforcement could understand. That is not to say that only State and local needed it. We needed it at the Federal level, as well.

What they came up with was this guide that has been distributed now, we have distributed nearly 100,000 of these to State, local, and Federal law enforcement, that quickly identifies high-tech evidence and how to safely seize that evidence without losing any integrity of that evidence. That is only the first step, but this was done as a concerted effort between State and local law enforcement agencies ranging in size from the Lubbock, Texas police department all the way up to the New York City police department. Every size department was involved in the development of this, was given the opportunity to provide comment and ensure that it was applicable to everyone involved in the initiative.

It was very effective. It is something that we have to continue to make sure that we are all dealing with these cases at the same level and sharing our experience and our training initiatives as much as we possibly can.

[The guide follows:]

Best Practices for Seizing Electronic Evidence

A joint project of the
International Association of Chiefs of Police
and The United States Secret Service

The *Best Practices for Seizing Electronic Evidence* was developed as a project of the International Association of Chiefs of Police Advisory Committee for Police Investigative Operations. The Committee convened a working group of a variety of law enforcement representatives, facilitated by the United States Secret Service, to identify common issues encountered in today's crime scenes. This manual was developed by representatives from the following agencies:

Alexandria, Virginia Police Department
Boston, Massachusetts Police Department
Baltimore County Police Department
Clarkstown, New York Police Department
Department of Justice – Computer Crimes and Intellectual Property Section
Florida Department of Law Enforcement
Florida Statewide Prosecutors Office
High Intensity Drug Trafficking Area (HIDTA) Program
Los Angeles County District Attorneys Office
Los Angeles Police Department
Lubbock, Texas Police Department
Maryland Heights, Missouri Police Department
National Association of Attorneys General
National Institute of Justice
National Sheriffs Association
New Jersey Division of Criminal Justice
New York City Police Department
New York County District Attorneys Office
New York State Organized Crime Task Force
Provo, Utah Police Department
Richardson, Texas Police Department
Rockland County New York District Attorneys Office
St. Louis County Police Department
United States Secret Service
Utah County Attorneys Office

Feedback!

If you have comment on this manual, please send it via email to
iacp_manual@usss.treas.gov

Best Practices for Seizing Electronic Evidence

Purpose

To develop a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media.

Introduction

Scope of the Problem

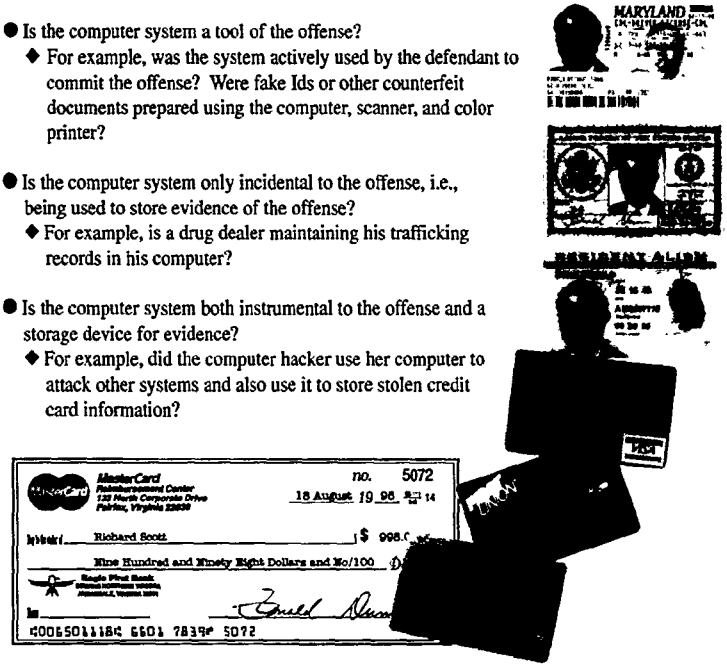
As computers and related storage and communication devices proliferate in our society, so does the use of those devices in conducting criminal activities. Technology is employed by criminals as a means of communication, a tool for theft and extortion, and a repository to hide incriminating evidence or contraband materials. Law enforcement officers must possess up-to-date knowledge and equipment to effectively investigate today's criminal activity. The law enforcement community is challenged by the task of identifying, investigating and prosecuting individuals and organizations that use these and other emerging technologies to support their illicit operations.

Recognizing Potential Evidence

Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband, fruits of the crime, a tool of the offense, or a storage container holding evidence of the offense. Investigation of any criminal activity may produce electronic evidence. Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant to the floppy diskette, CD or the smallest electronic chip device. Images, audio, text and other data on these media are easily altered or destroyed. It is imperative that law enforcement officers recognize, protect, seize and search such devices in accordance with applicable statutes, policies and best practices and guidelines.

Answers to the following questions will better determine the role of the computer in the crime:

- Is the computer contraband or fruits of a crime?
  - For example, was the computer software or hardware stolen?
- Is the computer system a tool of the offense?
  - For example, was the system actively used by the defendant to commit the offense? Were fake Ids or other counterfeit documents prepared using the computer, scanner, and color printer?
- Is the computer system only incidental to the offense, i.e., being used to store evidence of the offense?
  - For example, is a drug dealer maintaining his trafficking records in his computer?
- Is the computer system both instrumental to the offense and a storage device for evidence?
  - For example, did the computer hacker use her computer to attack other systems and also use it to store stolen credit card information?



Once the computer's role is understood, the following essential questions should be answered:

- Is there probable cause to seize hardware?
- Is there probable cause to seize software?
- Is there probable cause to seize data?
- Where will this search be conducted?
  - For example, is it practical to search the computer system on site or must the examination be conducted at a field office or lab?
  - If law enforcement officers remove the system from the premises to conduct the search, must they return the computer system, or copies of the seized data, to its owner/user before trial?
  - Considering the incredible storage capacities of computers, how will experts search this data in an efficient, timely manner?

Preparing For The Search And/Or Seizure

Using evidence obtained from a computer in a legal proceeding requires:

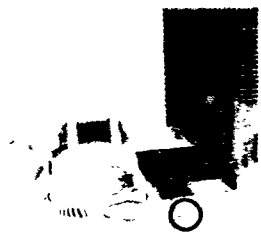
- Probable cause for issuance of a warrant or an exception to the warrant requirement.
  - Caution: If you encounter potential evidence that may be outside the scope of your existing warrant or legal authority, contact your agency's legal advisor or prosecutor as an additional warrant may be necessary.
- Use of appropriate collection techniques so as not to alter or destroy evidence.
- Forensic examination of the system completed by trained personnel in a speedy fashion, with expert testimony available at trial.

Conducting The Search And/Or Seizure

Once The Computer's Role Is Understood And Legal Requirements Are Fulfilled:

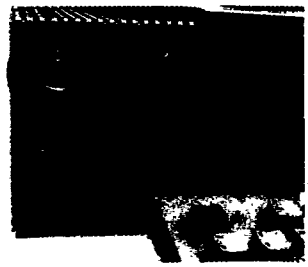
1. Secure The Scene

- Officer Safety is Paramount.
- Preserve Area for Potential Fingerprints.
- Immediately Restrict Access to Computer(s).
  - Isolate from Phone Lines. (Because data on the computer can be accessed remotely.)

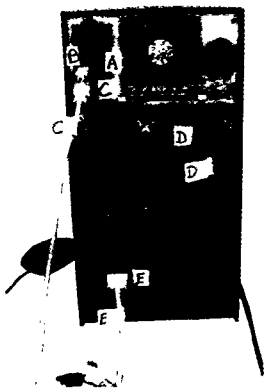


2. Secure The Computer As Evidence

- If Computer is "OFF," DO NOT TURN "ON"



- If Computer is "ON"
  - ◆ Stand-Alone Computer (Non-Networked)
    - ✦ Consult Computer Specialist



- ◆ If Specialist is Not Available
  - ✦ Photograph screen, then disconnect all power sources; unplug from the wall **AND** the back of the computer.
  - ✦ Place evidence tape over each drive slot.
  - ✦ Photograph/diagram & label back of computer components with existing connections.
  - ✦ Label all connectors/cable ends to allow reassembly as needed.
  - ✦ If transport is required, package components and transport/store components as fragile cargo.
  - ✦ Keep away from magnets, radio transmitters and otherwise hostile environments.

Networked Or Business Computers

Consult A Computer Specialist For Further Assistance

- ▼ Pulling the plug could:
  - ✦ Severely damage the system
  - ✦ Disrupt legitimate business
  - ✦ Create officer and department liability

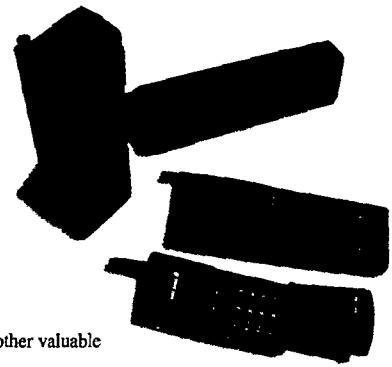
Other Electronic Storage Devices

Electronic devices may contain viable evidence associated with criminal activity. Unless an emergency exists, the device should not be accessed. Should it be necessary to access the device, all actions associated with the manipulation of the device should be noted in order to document the chain of custody and insure its admission in court.

I. Wireless Telephones

● Potential Evidence Contained In Wireless Devices

- ◆ Numbers called
- ◆ Numbers stored for speed dial
- ◆ Caller ID for incoming calls
- ◆ Other information contained in the memory of wireless telephones
  - ✦ Phone/pager numbers
  - ✦ Names and addresses
  - ✦ PIN numbers
  - ✦ Voice mail access number
  - ✦ Voice mail password
  - ✦ Debit card numbers
  - ✦ Calling card numbers
  - ✦ E-mail/Internet access information
  - ✦ The on screen image may contain other valuable information



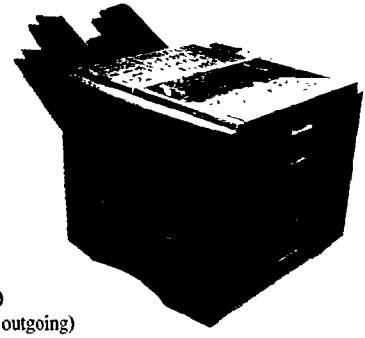
● On/Off Rule

- ◆ **If the device is "ON", do NOT turn it "OFF"**
  - ✦ Turning it "OFF" could activate lockout feature
  - ✦ Write down all information on display (photograph if possible)
  - ✦ Power down prior to transport (Take any power supply cords present)
- ◆ **If the device is "OFF", leave it "OFF"**
  - ✦ Turning it on could alter evidence on device (Same as computers)
  - ✦ Upon seizure get it to an expert as soon as possible or contact local service provider
  - ✦ If an expert is unavailable, USE A DIFFERENT TELEPHONE and contact 1800-LAWBUST (a 24 x 7 service provided by the cellular telephone industry)
  - ✦ Make every effort to locate any instruction manuals pertaining to the device

II. Electronic Paging Devices

● Potential Evidence Contained in Paging Devices

- ◆ Numeric Pagers receives only numeric digits (can be used to communicate numbers and code)
- ◆ Alpha Numeric Pagers (receives numbers and letters and can carry full text)
- ◆ Voice Pagers (can transmit voice communications (sometimes in addition to alpha numeric)
- ◆ 2-way pagers (Containing incoming and outgoing messages)
- ◆ Best Practices
  - ✦ Once pager is no longer in proximity to suspect - turn it off. Continued access to electronic communications over pager without proper authorization can be construed as unlawful interception of electronic communication
- ◆ Search of stored contents of pager
  - ✦ Incident to Arrest
  - ✦ With probable cause + exception
  - ✦ With consent



III. Facsimile Machines

● Fax machines can contain:

- ◆ Speed dial lists
- ◆ Stored faxes (incoming and outgoing)
- ◆ Fax transmission logs (incoming and outgoing)
- ◆ Header line
- ◆ Clock setting

- **Best Practices - Fax Machines**
  - If fax machine is found "ON"
    - Powering down may cause loss of last number dialed and/or stored faxes

- **Other Considerations**
  - Search Issues
    - Record telephone line number fax is plugged into
    - Header line should be the same as the phone line . . .user sets header line
    - All manuals should be seized with equipment, if possible

IV. Caller ID Devices

- May contain telephone and subscriber information from incoming telephone calls
  - Interruption of the power supply to the device may cause loss of data if not protected by internal battery back up
    - Document all stored data prior to seizure or loss of data may occur

V. Smart Cards: A plastic card the size of a standard credit card that holds a microprocessor (chip) which is capable of storing monetary value and other information.

- **Awareness**
  - Physical characteristics of the card
  - Photograph of the smart card
    - Label and identify characteristics
    - Features similar to credit card/driver's license
    - Detect possible alteration or tampering during same examination

- **Uses of Smart Card**
  - Point of sale transactions
  - Direct exchange of value between cardholders
  - Exchange of value over the Internet
  - ATM capabilities
  - Capable of storing other data and files similar to a computer

- **Circumstances Raising Suspicion Concerning Smart Cards**

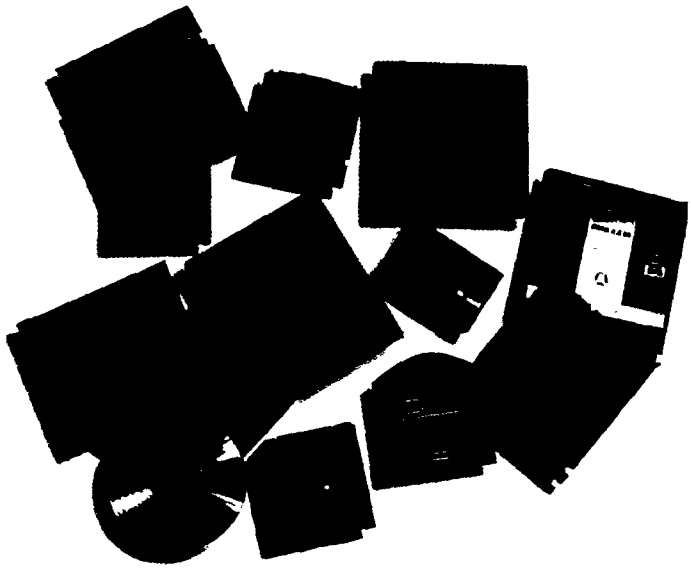
- Same as credit cards
- Numerous cards, (different names or same issuing vendor)
- Signs of tampering
  - Cards are found in the presence of computer or other electronic devices

Questions to Ask When Encountering Smart Cards

- Who is card issued to (the valid cardholder)?
- Who issued the card?
- What are the uses of the cards?
- Why does the person have numerous cards?
- Can this computer or device alter the card?

Other Considerations

- Smart Card technology is used in some cellular phones and may be found in or with cellular devices(See Wireless Section)



Tracing an Internet Email

- When an internet e-mail message is sent, the user typically controls only the recipient line(s) (To: and Bcc:) and the Subject: line.
- Mail software adds the rest of the header information as it is processed.

Reading an email header:

Sample Email Header

```
                    -----Message header follows-----
(1) Return-path: <ambottom@in50210.cc.nps.navy.mil>
(2) Received: from in50210.cc.nps.navy.mil by nps.navy.mil
    (4.1/SMI-4.1) id AA08680; Thur, 7 Nov 96 17:51:49 PST
(3) Received: from localhost by in50210.cc.nps.navy.mil (4.1/SMI-4.1)
    id AA16514; Thur, 7 Nov 96 17:50:53 PST
(4) Message-Id: <9611080150.AA16514@in50210.cc.nps.navy.mil>
(5) Date: Thul, 7 Nov 1996 17:50:53 -0800 (PST)
(6) From: "Albert M. Bottoms" <ambottomin50210.cc.nps.navy.mil>
(7) To: Tim White <ti white@$m.ir.lo.COM>
(8) Cc: Real 3D <real3d@mmc.com, Denny Adams <dadams@ldsa.com,
    Tim Arion <tarion@aol.com>, RAY BALCERAK <RBALCERAK@AR'A.mil>
```

- **Line (1)** tells other computers who really sent the message, and where to send error messages (bounces and warnings).
- **Lines (2)** and **(3)** show the route the message took from sending to delivery.
  - ◆ Each computer that receives this message adds a Received: field with its complete address and time stamp; this helps in tracking delivery problems.
- **Line (4)** is the Message-ID, a unique identifier for this specific message. This ID is logged, and can be traced through computers on the message route if there is a need to track the mail.
- **Line (5)** shows the date, time, and time zone when the message was sent.
- **Line (6)** tells the name and e-mail address of the message originator (the "sender").
- **Line (7)** shows the name and e-mail address of the primary recipient; the address may be for a:
  - ◆ mailing list,
  - ◆ system-wide alias,
  - ◆ a personal username.
- **Line (8)** lists the names and e-mail addresses of the "courtesy copy" recipients of the message. There may be "Bcc:" recipients as well; these "blind carbon copy" recipients get copies of the message, but their namesand addresses are not visible in the headers.

Mr. SCHNEIER. You can hardly go to a hotel, even a Holiday Inn, these days without having access for your computer. Many of the members that I represent here spend most of their time on the road, traveling, and they are increasingly using their computers from these remote locations.

Do they face any greater level of risk because they are working from these remote locations and maybe dealing with a local network out of their personal residences or out of some other location?

Mr. FARNSWORTH. Generally speaking, folks who move around like that and log in from remote locations are issued a new network address each time they log in, which makes them significantly less vulnerable, I would say. However, the fact that they are logging into a central location makes that central location more vulnerable because it has to be set up in order to accept communication calls.

So there is a double-edged sword there. Certainly, take protections on the individual laptops to make sure that if they are compromised electronically, lost, or stolen, that the information that they contain is protected. Local cryptography programs can help you with that. Virtual private networking tools can assist with that.

But more importantly, look at the site to which they are dialing and make sure that you have a strong authentication mechanism in place to make sure that the connections coming in are, in fact, from legitimate users.

Mr. LANE. A lot of businesses for the sales reps that are out there are buying the high-speed modems because they are transferring a lot of information, which gets back to: Are they leaving them on all the time? So all of the sudden, that information becomes critical because what they do is they dial into your system and then they are able to get all that information and then dial back to the central server with all the information intact. You then totally compromise the site, no matter what you have done at the central site to begin with.

So you need to, again, educate those individuals that if they have open lines all the time, they should close them down. The businesses that are supplying them with the technology should have the firewalls in place, both in the laptops and in the system.

Mr. CHARNEY. I would like to point out, your question reveals how difficult this is, particularly for small businesses. It is absolutely true, if you have got a lot of mobile people with laptops you want to protect their data. But you can educate your users so if one of your users said, "I really want to protect my data in case my laptop is stolen from the hotel. So I am going to encrypt all my data." This is a good thing to do.

Then he goes out, he follows 20 sales leads, gets lots of information, he encrypts all that data in case his laptop is stolen, and then he gets hit by a bus. The laptop is given back to the company, and they cannot get any of the data because he encrypted it.

Therefore, if you are going to use encryption, now you have to think about key recovery. What kind of encryption are you going to use that if the employee either goes bad or just has some sort of accident and is unavailable, the company can gets its data back? That is part of the problem, none of this stuff is simple. And for

small businesses, it is very hard to find people who would think: We need an encryption scheme with key recovery so the company can be protected, and then we have to implement it, educate users, and manage the keys. It is not easy.

Mr. SCHNEIER. I was feeling better there for a moment.

Mr. DOZIER. Mr. Charney, then in light of your comments, what do we do to protect consumer confidence? I do not necessarily mean just consumers purchasing from small businesses, but small businesses also purchasing from their suppliers. From what we have heard today, the rate of incidents are going up. From what we have heard today, there is an overlap of enforcement mechanisms. From what we have heard today there is not really a one-stop shop, in terms of going to one place to make a complaint or to say that your system has been compromised in some sort of way.

The Internet is a lot like the dollar bill. There is nothing behind it, we just have confidence in it because people say it is worth something.

So what do we do, and what do the representatives around the table do to protect that consumer confidence in the Internet? To say that this is a safe place to shop, this is a safe place to purchase, this is a safe place to transact?

Mr. CHARNEY. I think there are two things, there is reality and perception, and both are important. On the reality side, I think small businesses, through their associations, need to continue their dialogue with vendors about how to have security built into products that are easy to implement. So, when you look at browsers today that use secure socket layer, for example, if you build that stuff into the products and consumers can use their credit card on the Internet, it will be encrypted from their home machine to the merchant, and that works seamlessly. Because it is deployed in the product, it is very cheap and it is spread out over the whole group. So there are some real basic security things that can be done by the vendors.

The perception is a separate problem. People will not use the Internet if they perceive it is not secure, even if it is secure.

Mr. DOZIER. The Committee has held a lot of forums and we have heard from small businesses that said they are terrified of the Internet. We have seen a lot of fraud schemes and I think we investigated that at one time. We also talked about barriers, in terms of people wanting to get on the Internet and transact, whether that be importing or exporting to other countries.

So we are very concerned about basically how safe it is.

Mr. FARNSWORTH. Let me just speak to that very quickly. The chart that shows the number of incidents spiking there is a very frightening chart. But if you overlay that with the chart that shows the overall growth of the Internet, your perception changes.

Mr. DOZIER. So the percentages are actually down?

Mr. CHARNEY. No, level.

Mr. FARNSWORTH. And the thing is, despite personal occurrences and the traumatization that they cause, it is statistically very improbable that someone will be attacked on the Internet.

I also want to point out, while we talk about law enforcement efforts and the efforts to get information to people about who to go to, many of our educational efforts in the past that dealt with tra-

ditional crime in brick-and-mortar institutions dealt with educational programs to say leave a light on, trim the bushes back away from the windows, get an alarm that is centrally monitored.

These are all good ideas in cyberspace, as well. The idea here is not that if you are turning the light on and locking the door and trimming the bushes back and a burglar comes down the street, your intent is not to cause that person to look inside themselves and say. "I do not want to be a burglar anymore." Your intent is for them to say, "Oh, this guy has got a dog, the house is lit up, there is a sign from an alarm company. I am going to go around the block and see if there is an easier target."

Small businesses, if they stay in the herd, implement best practices, and take a responsible approach to Internet security, can be safe as a herd. It is when you overlook these things that you become statistically more prone to these types of attacks.

Mr. CHARNEY. We have to remind consumers that the physical world is a dangerous place, too. They may get carjacked or have a car accident and they do not give up their car. When consumers say they do not want to use their credit card on the Internet, what we used to say to them is, "Well, do you give it to the waiter in the restaurant?" What does he do? He goes in the back with it. OK, so what is your concern?

I mean part of it is really an educational problem.

Ms. NEPTUNE. Is it not also true that most of the credit card crime is not from them sending it to buy things, but where all of the credit cards are stored? So even if you called up and gave them your credit card, they would be under the same amount of risk. So it is really not sending it.

Mr. FARNSWORTH. That is right. The actual transmission of the card data, whether it is encrypted or not, the odds of intercepting that particular transmission, putting the numbers in order, and getting useful information from that is just infinitesimal, given the volume of traffic that is going over the electronic media every day.

Mr. MORRISON. It seems to me, from what I know of this, that some of this problem is rooted in the genesis of the Internet as a way mostly for universities to communicate to one another. The notion of commerce going over the Internet was not even really thought of as part of the picture, when the system was created.

We are now hearing about a successor network and, maybe in 2003 or something, Internet II. Is it possible to engineer better security into a successor network? And what might we look forward to in that respect?

Mr. FARNSWORTH. Absolutely. Actually, a lot of the work that is going into the next generation Internet protocol is being retrofitted into our existing infrastructure today, and concepts that include digital authentication or certification of users and encryption or authentication of traffic actually had been developed for deployment in the next generation infrastructure and is being employed in today's networks.

Your comment about the size, when the Internet was designed we were talking about tens of hosts and communicating largely between military and educational facilities. Today we have, I believe, over 40 million hosts connected to the Internet.

So the foundation which was built to facilitate open communication is being stressed severely in that space. What we have seen is a large amount of entrepreneurial spirit on the part of small businesses to come up with products like firewalls, which are extremely useful in this space. Those companies, there are several that I can think of right off the top of my head, who have been wildly successful at deploying that technology. I think that is going to continue. It will be innovators and small organizations that are very bright and can evolve these products who will fill the need until the next generation infrastructure can be deployed.

I think it is also important to point out that whatever we deploy for the next generation infrastructure will probably have an equally long lifetime. So making sure that that infrastructure supports sophisticated security mechanisms as an integral part of its evolution is important.

Ms. RILEY. I think from the law enforcement perspective, and having chased some of the activity around, I have to emphasize, too, though the consistency and the completeness of that type of security. While the network and certain offerings can certainly add more security features and allow for more consistency between the users of the Internet, if the entire security package is not reviewed, the holes are still going to be there.

I think, Mr. Lane, you made the point that it is a process. If you have all of the security and all the encryption built into your computer, but you forgot to lock the front door on your way out, the vulnerability remains. So the emphasis has to be placed on the issue that we need to be consistent in the types of security mechanisms that are being deployed, so if one place plugs the hole and the other one leaves it open, we are not gaining anything there.

And that those that are deploying security are looking at it as a complete issue and not focused only on the network, but on all the components of security associated with their business.

Mr. PAGE. Mr. Charney, you mentioned earlier in your testimony that there is what you called a lack of talent, or that there is a drain in talent? Do you have a proposal or suggestion to the panel here, to the Small Business Committee, or even the Small Business Administration that would help assist small businesses that are starting to wade into the Internet who are using the Internet commerce as a means of educating their staff or whoever is in that small business, and it may even be a part-time employee, who all of a sudden takes on the systems administration responsibilities. What can we be doing to better educate these employees who ultimately hold the keys to security to the business?

Mr. CHARNEY. There are a couple of things that both businesses can do and that the Governments have to do. On the business level the problem is one of cost. In the early years, when I started doing computer crime, you found that many system administrators were secretaries who were really good at word processing. When it came time for someone to manage the network they said, "You are really good with your computer, you are now the systems administrator." And she would say, "That is great. What is that?"

Then when you talked about doing it right it meant OK, you have to start taking training courses. You may have computer literacy and you are not computer phobic, but you need to go take

courses. There are lots of them by lots of organizations. You can take courses from the CERT team at Carnegie Mellon on how to do emergency response and set up a computer emergency response team within a company.

The difficulty is for a small company that is a large resource drain. You are going to take someone and give them 80 hours of training at the start. Then because the technology changes, like in my company, constant training is required. Every year people have to go back and back and back. Windows 2000 is out. OK, time to go get Windows 2000 training.

So it is very, very difficult for a small business to say, "Not only are we going to tell you that you are the systems administrator, but at the same time we are going to allow you all this funding to take training and the time to take the training," which means that employee is out-of-pocket. But companies do need to do that.

The second thing is we have to increase the supply of technically literate people. There are some proposals to do that now. For example, the Government is looking at an ROTC-like program for systems administrators. The Government will pay for your education if you get your degree in computer security, and then devote 4 years to computer security. That is just one example.

But the supply/demand ratio is way out of whack. That not only means you cannot find talent, but what talent is there is very, very highly priced talent. So it is very hard for smaller companies to grab that talent.

Mr. FARNSWORTH. Along with that, what we have seen is a redeployment of that talent. It used to be that the folks who knew what they were doing with security would not only set the policy, but would be responsible for implementing and managing that policy, to the point where they would be behind the keyboard making rules changes to firewalls and access control on the infrastructure.

What we are seeing now is a redeployment of talent and a new generation of products. For example, products that Cisco has brought to market that allow the network management people who are already doing things like the telecom and links management to actually take the steps to enforce policy. And the people who are aware of information security technologies become sort of the mentors and the policy setters who state what needs to be done and the dates by which it needs to be done.

So what we are seeing is that the centralization of these resources, and the people who know what they are doing, moving to more strategic roles within organizations.

Mr. CHARNEY. And somewhat of an automation of the process, as well. I have a client, for example, who can have his servers reach out to a main server and give a little command. Then the main server will attack the servers and do attack and penetration and check settings and do all this stuff in an automated way. It is not foolproof by a long shot. The technology is a bit too complex to automate the whole process. There needs to be some intuitive human intervention. But you will see more automation, I think, of security to take it out of the hands of the people.

Ms. NEPTUNE. That would help, because even if you train people and you give them all that, you know in a year you are going to

lose them because they are going to get a fantastic offer from somebody else.

Mr. LANE. This ties in to a more controversial issue which is the whole H1–B visa issue. I mean, if you lift the caps of H1–Bs and you allow technically literate people to come into the United States, it helps fill some of the gaps that are out there. So it is very important for small businesses to support the lifting of the caps on the H1–B visas.

In addition, technology does provide security. There is a new company out there that has developed, for lack of a better system, a credit card system that is the size of a credit card but fits on your CD–ROM. What it does is it sends encrypted information to the business with your account information, but the business does not collect that information. What the business does is it forwards it to the bank and the bank decrypts it and then wire transfers the money back to the small business or the large business, depending on the clientele.

So that way, the issue of security of credit cards is not compromised because it is at the host which would be the bank, which supposedly would have the best encryption and the best security mechanisms and serve the small businesses, without having the liability of holding these credit card numbers on their site.

So technology again is working to try to help small businesses.

Mr. DOZIER. What type of internal controls are available to a small business, or a large business for that matter? I mean in the context of let us say you have a disgruntled employee or something, who then could take the password and sell it at a profit, or just corrupt the system because they are having a bad day. In my thinking, that is a form of crime as well.

So what can a business do to sort of protect its assets internally, as well as externally?

Mr. CONLON. Can I just jump in and say something on that? In a prior life, before coming up here, I worked for a technology company where we used to see people attempting to get at the accounting servers in the company on a daily basis. It never ceased to amaze me.

This is related to Damon's question, the insider angle. You know, threat from inside.

Mr. Charney.

Mr. CHARNEY. Clearly, the insider threat is larger than the outsider threat. That is absolutely true. The reason for that is you have given insiders access to your systems, so they do not have to break in.

There are reasons the outsider threat gets more attention, and we can talk about that later. But there are internal controls in businesses that have been used in the paper world that also work in the technical world. Basically what you need to do is a combination of personnel security, physical security, and IT security. And you need to monitor systems for anomalous transactions.

You cannot necessarily stop a secretary or an employee from giving their password to a bad guy, but you can require that passwords be changed regularly and you can monitor the use of the password. So for example, if you see that someone is dialing in and

using this password and the employee is also logged on internally with this password, you know instantly you have a problem.

Mr. DOZIER. But is that not sort of crossing the line, in terms of the privacy issue we raised before? I mean, I understand that there are certain keystroke programs that you have where you can watch every key stroke. But do you not get into a situation where you are having very, very aggressive oversight of your employees, if you are watching every step that they take?

Mr. CHARNEY. First of all, it depends on what you are watching. I think most employees expect that businesses will keep logs of who signs on and that their user names and passwords are valid. Those do not raise the same kind of privacy concerns as, for examples, reading employees' e-mails, especially when you have told employees that short personal messages are OK and you reserve the right to read them.

Now under Federal law, the Electronic Communications Privacy Act, in fact, companies can read electronic mail. It does not violate the wiretape statute. Although some employees have sued for invasion of privacy in State courts, they have generally lost those suits and the courts have held that businesses do have a right to protect their business interests by monitoring the activities of employees on their own network.

It is more complicated for businesses that are offering services to the public because monitoring of public activities, and particularly things like chat rooms where you have huge first amendment interests, obviously raise a different level of concern than it does when you tell employees—and I wrote the Justice Department monitoring policy for the criminal division—when you tell employees, "Look, we have an obligation to make sure that Government equipment is used for Government purposes and we reserve the right to watch what is happening on our networks." Most employees are fine with that.

The key is notification and education so they do not feel they are being surreptitiously monitored, which creates a ton of bad morale.

Mr. SCHNEIER. Ms. Neptune, you mentioned in your presentation that your insurance carrier was helpful to you. Was this coverage part of your normal liability package? Or was this something that you had to buy in addition? And is it something that most small business owners should be looking at?

Ms. NEPTUNE. We had a very extensive insurance policy. You know, with the Internet now, every year there was a new policy you had to do. Computer fraud, copyright, patent right, because I had a site service. It was very expensive, but I happened to purchase business-income loss, which as we all know is a very expensive policy. If I did not have that, I would not have gotten any reimbursement.

Mr. SCHNEIER. But was it an additional rider that you had to get?

Ms. NEPTUNE. Yes, it was because it is not covered under normal theft. It is specifically for loss of business income. It kicks in based on how much you want to pay. Do you want it to kick in in 10 hours, 24 hours, a certain level or whatever? And these are very expensive.

I might also add, we were cancelled the next year, of course, from the insurance carrier. Now go find it from somebody else. So it has a rolling effect.

Mr. CONLON. Mr. Farnsworth and Mr. Charney, I will direct this one to both of you. How much does all of this cost? There are a lot of incidents going on, some of them are reported, a lot of them are not. Is there any kind of ballpark figure of how much this costs the business world?

Mr. FARNSWORTH. There is a wide range of solutions with a wide range of costs. What we have found is that it is very much, as we just heard about the insurance industry, folks are more likely to spend more money if they have been victimized than if they have not been. Small businesses can subscribe to services from service providers who take advantages of economies of scale to provide secure web hosting, secure content hosting services at a reasonably low cost.

Businesses who are engaged in controversial business practices, if you make baby harp seal fur coats, for example, there is some segment of the population that might take exception to that, thus raising your visibility and your vulnerability. Those folks will necessarily have to spend more money in order to protect their resources.

You can get something as simple as a personal firewall software package for $20 to $30 and download it over the Internet. You can go as high as hundreds of thousands of dollars to provide state-of-the-art high-capacity firewalling with intrusion detection and centralized-monitoring services. It is a risk assessment and risk vulnerability issue, though.

Mr. CHARNEY. If you are talking about the cost of computer crime generally, several years ago I started looking at the public literature. The public literature ranged from computer crime is costing businesses $50 million a year to $5 billion a year, which basically tells you that no one has a clue. I mean, you can discount the high-end one as lunacy. But if you look at the CSI surveys, they try and quantify the cost. But if you remember that most computer crime is not detected nor reported, it is really hard to get an accurate figure.

Mr. CONLON. We included the computer security study in the packets we distributed.

A question for Agent Riley. Mr. Charney, in his testimony, talked about the kind of impact on, I believe it was a bank, that had suffered a computer crime when you have to go public with this. And the same kind of issue with Ms. Neptune, with reduced consumer confidence.

How much of a challenge is this to law enforcement? And what has law enforcement been doing to kind of get over the issue of consumer confidence and confidentiality.

Ms. RILEY. That is a good question. As I pointed out earlier, when we train agents to work CyberCrime, we train them not only in the technical aspects of how to follow the leads and how to work through to an investigation, but we also focus very heavily on the impact of any publicity and any actions by law enforcement, and how that will affect the victim after we come into the scene.

I cannot emphasize enough that all of the work that was done on the investigation that was described for you this morning was done in partnership. I think Ms. Neptune will certainly agree that everything that was done associated with that case was discussed at great length with both the law enforcement representatives, the Secret Service agents from the local Miami field office, along with the company, so that we could explore any actions that we might take and the resulting impact that is there. I cannot emphasize those partnerships enough, before, during, and after the investigation.

As far as publicity goes, within our own agency we have a very strict policy, which is that no press releases are put out about any investigations by our agency. Rather, that is done by the United States Attorney and the prosecutor's office. At times there is a careful balance that is weighed there.

At certain times, the publicity associated with the case may more importantly come from the Government or the prosecutor and put the perspective on the case and the way that it was worked out rather than a defense attorney, for example. So publicity is not always bad. It also serves as a deterrent factor, to put the word out that you can be caught when you do these types of investigations.

But again, as was done in the Boston case, where the telephone companies were heavily victimized, they actually participated in the press release. The message that they wanted to get across as a victim was that we are not going to tolerate this type of activity.

So I think there is good and bad associated with the type of activity we have to do in releasing information about an investigation, but it is very important that we consider the partnerships with the victim and with the other affected industry members when trying to weigh how to release information about an investigation.

Mr. CONLON. If there were a single message from law enforcement to the participants around the table here, what would that be? Something that they can take back to the members of their associations.

Ms. RILEY. I actually would have to support the comments made by several of my colleagues here on the panel, which is share information. The prevention is really a key. Preventing this type of activity by sharing information, we are happy to do that from the law enforcement perspective, especially with trade associations. Ms. Neptune made a great point, the trade associations give us a mechanism in law enforcement to share that hindsight with larger segments of industry and try to effectively help in the prevention techniques.

The types of techniques or the tips that were provided by Mr. Farnsworth today, for example, we absolutely support the initiatives underway within industry to prevent these types of crimes. But when they do occur, we have got to learn from those. And we are committed, in law enforcement, to help industry do that.

Mr. CONLON. I believe Senator Bond will be returning in a few minutes so I guess we will take the opportunity to wrap up. Mr. Lane has a comment?

Mr. LANE. Consumer confidence is critical to small businesses when you are getting onto the web as a small business. I have

started my own software company. It is four guys sitting around a table deciding to come up with a product. The best thing to do is try to get eyes to your sight or get consumer confidence in the product that you are developing.

But what is really hurting us right now is, I hate to say it, but the press focusing on a small amount of cases. Even the title of this forum, "CyberCrime: Can Small Business Protect Itself?" sends out a message that my god, I better not go to the small businesses. I better go to the Amazon.coms of the world who are, in fact, being attacked.

We have to make sure that we are not sending out a message of fear that inhibits the ability of the Internet to grow. Just like any business, consumers go into places where they feel comfortable. They go into the stores where they feel comfortable. Small businesses have to work to build up consumer confidence, but it does not help when we have a fear factor for either political reasons and we say, "Oh my gosh, we need to do something and vote for me next November," or something else.

We need to make sure that we are providing quality information out there, which gets back to the other issue of sharing information. On the Y2K example, the Y2K liability was a perfect example for businesses to share. There were a lot of antitrust issues that businesses could not talk to one another and share information about because of antitrust concerns. What do we do about that? How can we allow the sharing of information?

Then on the association side, if we put out information and it is inaccurate, are we now liable? Again, the Y2K liability and the legislation on the Y2K sharing of information took care of that. But we need to look at this as a whole because right now we are not going to put anything up on our site that makes us liable. We cannot ask our businesses to talk to one another and say you are not going to be slammed by an antitrust suit.

So we need to look at all this, plus the FOIA information that is out there, as well.

Mr. BURTON. I just want to take a minute just to completely underline what you said from the viewpoint of direct marketing, not only in terms of liability which is something of very great concern to us that we want to try to work around it, but probably more than almost any type of business, direct marketing depends on consumer confidence. We have, since the beginning of the Sears Roebuck catalog, had to depend on arms-length transactions where you do not know the people you are dealing with and you have to trust the process.

So we have had a lot of experience before the Internet even came in trying to create a trust process. It is totally and absolutely critical that we have a process we can trust.

I agree, though I do not like to attack the media in any way, I agree that I think that from a consumer perspective the problem has been overdramatized. In other words, I feel perfectly safe, much safer conducting business on the Net with companies that I know or at least can trust, than I do giving it to a restaurant.

In fact, I have had my identity stolen twice. Once it went all the way to Paris. In both of those cases it was because of a waiter in

a restaurant. I have never been to Paris, but my credit card has been there.

So I just want to underline that I think that forums like this are very, very important. We, of course, commit ourselves, to working with law enforcement officials and people who provide security on the Net, so that we can be sure that we have this consumer confidence. Because the wave of the future is going to be buying on the Net.

Mr. DEBOW. I concur that there are a lot of positive things that we can compliment, particularly law enforcement and all the different organizations that are working hard to try and keep pace. But one of the things that I feel we would be remiss if we did not consider is that there is a tremendous marketing assault to get those people which may have been considered to be technologically phobic, or, for whatever reason not accessible to the Internet, to come to the Internet.

I think when you look at these major corporations that are practically giving away computers to their employees, you have got products now that are designed in the $100 price range to be particularly directed towards the Internet. There are a lot of things which we can anticipate which would probably be somewhat of a repetition of things we have already identified. There are areas that need to be prepared for and anticipated including an exchange of information or some type of educational process.

One of the things that, in our particular organization, which is the National Black Chamber of Commerce, which we are being questioned about and are confronting is a reverse side of the caveat emptor aspect of the card services providers—in that when there is a dispute or something that is questionable, where the consumer wants to challenge the charge on the credit card, those companies traditionally immediately either freeze those funds that are in that merchant's account, or they are immediately removed. There are basically, I think, two major companies that are providing that service. They go about the judicious process of determining whether it is a valid dispute, or perhaps maybe the consumer did use the product and just chose not to want to keep it or whatever.

The education and information to other small businesses, which probably is going to be an ever increasing density of the existence of those businesses as well as these type of circumstances where they do, in fact, feel somewhat defenseless in their ability to protect the sale because they have, in fact, shipped the goods or provided the services. It is gone from their inventory. It is gone from their business. And now the funds and the reciprocal for that are in question.

So with that in mind, is there a place: (1) where we can go and see some type of statistics on consumer satisfaction or dissatisfaction with these particular companies? And (2) what do you do if you feel you have been unjustly dealt in one of those circumstances? I would just throw that out to anybody.

Mr. LANE. The problem with online transactions is that the company is responsible. It is not reimbursed by Visa or Mastercard or American Express, the $50 limit. The business itself, because it is unsigned, eats that cost. So there is a huge incentive to try to make sure that that is a valid transaction.

That is the way it is for a phone call, anything where there is not an underlying signature of a transaction. So there is a huge concern for small businesses.

We heard last year from a small business that sold lobsters from Maine. The problem with that is you cannot return the product. It is either eaten or it has been dead for too long and you cannot resell it. They were estimating almost 30 percent of their sales were in conflict, people saying we did not receive it or saying that we did not like it or trying to dispute it. The company had to eat those costs. So it is a huge risk to businesses. I do not know what the underlying answer is, but it is real.

Chairman BOND. That is something we are going to work on. I know we have reached the hour we said that we were going to close.

First, I want to express my sincere thanks to all of you for participating today. Obviously, this is a question of great importance, not just for small business but for everybody involved in e-Commerce. I want to offer a special thanks to the panelists for joining us, for providing what my staff tells me has been very interesting and informative testimony. We have had some great insights into what the real life problems are.

There is no question that Government can provide a lot of information that will be of assistance to the small business community. I think that is something that we need to explore and we will continue to work on that.

But there is one question, I guess, that has kind of floated around without an answer and I have a suggestion that I am going to propose. What does a small business do when they have been hit? Who do you call? What is the 911 if you find out there has been a problem? Obviously, Ms. Neptune was able to get in touch with the Secret Service.

I propose to write to FBI Director Louis Freeh to ask him to ensure that the National Infrastructure Protection Center undertakes outreach initiatives to the small business associations around this table and to small business generally, to Government-funded business development programs, to Small Business Development Centers, the Business Information Centers, and the Service Corps of Retired Executives who were unable to join us today.

I will be writing to Attorney General Janet Reno to request that a toll-free number be set up to provide a single point of contact for small business consumers and others to report computer crimes and computer security issues related to law enforcement. We have seen a similar system in the FTC with the toll-free number, 1–877–FTC–HELP, which I think has provided small businesses with good access to information, and given business owners a place to go.

I think that given the overlapping jurisdictions of the various law enforcement organizations, it is important that some centralized entity provide a common point of contact for small businesses and others to reach law enforcement organizations. We will work with you and would like your comments and suggestions on that.

Obviously, this is a subject which we have just begun to discuss. We intend to continue to work with it, Paul and Damon and our Committee Members' staffs here, along with you as we determine how best we can deal with the problem. As we can see, the problem

is rising. As Mr. Charney said, it may be rising a whole lot faster than we even know.

I think that the time has come, if not even past, for us to be serious about providing some comprehensive assistance. I know the private sector, Mr. Farnsworth and others, are working to assure that we have the technology and the equipment. We do not want to do anything that would interfere with the ability of the industry and all the related organizations to develop appropriate response mechanisms. That is where we need your guidance.

How can you all handle it best through technology? To the extent that there is Government assistance needed, we would like your advice and counsel on that. You have given us a lot of good ideas to follow up.

Again, my sincere thanks to all of you for joining us today, for discussing what is emerging as a very serious problem, particularly for a lot of small businesses who may not realize that they are at risk. As always, you have been very helpful and I appreciate the time and the information that you have presented us.

Thank you very much and the hearing is adjourned.

[Whereupon, at 11:42 a.m., the forum was adjourned.]

COMMENTS FOR THE RECORD

The National Association of
Government Guaranteed
Lenders, Inc.

Statement

of

Anthony R. Wilkinson

President
and
Chief Executive Officer

of the

National Association of
Government Guaranteed Lenders, Inc.

for the

Committee on Small Business

United States Senate

February 24, 2000

Post Office Box 332 • Stillwater, Oklahoma 74076 • 405/377-4022 • FAX 405/377-3931

Mr. Chairman and Members of the Committee. My name is Tony Wilkinson and I am President and Chief Executive Officer of the National Association of Government Guaranteed Lenders, Inc, or NAGGL. NAGGL represents nearly 700 lenders and other program participants who make approximately 80 percent of the 7(a) loans guaranteed by the Small Business Administration. We thank you for holding this hearing today and requesting our input on SBA's budget and proposed authorization levels for the 7(a) program.

7(a) Budget and Authorizations

First, let me raise a problem with this year's budget. The current appropriation supports a fiscal year 2000 program level of approximately $9.8 billion. We believe that loan demand, which historically is higher during the spring and summer months than in the winter, will be $10.5 billion net. We have discussed this shortfall with the Agency, but SBA has not announced its proposal to correct the problem. We would hope that they would do so very soon as the necessary corrective action becomes more acute due to the shorter time remaining within the fiscal year to implement it.

Second is the 2001 request. We agree with SBA's request of $11.5 billion net, which is the amount of demand we estimate for next year.

Third, as to authorizations, we recommend that the Committee continue its past policy of providing three-year authorizations. Specifically, NAGGL recommends the following authorization levels in amounts of 7(a) loan guarantees:

- $14.5 billion in fiscal year 2001,
- $15.0 billion in fiscal year 2002, and
- $16.0 billion in fiscal year 2003.

We would note in this regard that NAGGL is recommending straight-lining the authorization level from the year 2000 to the year 2001 as Congress has already authorized a $14.5 billion program level for fiscal year 2000. We believe that these amounts are sufficiently above the current budget level to provide some flexibility to the Appropriations' Committee in future years should a change in the economy necessitate consideration of a higher level of loan guarantees without the necessity of the authorization being changed.

7(a) Program Performance

We were pleased that the President's Budget Request reported that the 7(a) program performance remains high: the recovery rate on liquidation of defaulted loans remains unchanged in 2001 at 60.6% while the default rate is projected to decrease slightly from 14.42% in 2000 to 14.29% next year. I am compelled to say, however, that NAGGL believes that the default rate is still materially overstated.

As part of the subsidy rate calculation, SBA each year looks back to see how the actual numbers compared with the projections and re-estimates or calculates the difference. As of last year, the costs were projected too high and resulted in a re-estimate that the Agency had collected $833 million more than was needed. The 2001 Budget Request reports more of the same: another $176 million excess.

In essence the 7(a) program is operating at a profit to the government under the current fee structure! It should not have any subsidy cost and fees should have been reduced rather than needing to appropriate money to pay for the program. The 7(a) program more than pays for itself, but the erroneous assumptions mandated by the Office of Management and Budget continue to prevail.

Subsidy Rate Floor

At this point I would request the Committee's indulgence in addressing a topic that we refer to as a subsidy rate floor.

In 1994, SBA began using a new subsidy rate model and in order to offset the model's projections of the cost of operating the 7(a) program, this Committee imposed a very substantial increase in 7(a) guarantee fees. Until this increase in fees was imposed by Public Law 94-306, borrowers paid a one-time fee of 2%. The new law retained that fee only on loans of up to $80,000. Larger loans incurred higher fees, some almost doubled:

- 3 percent on the first $250,000 guaranteed,
- 3.5 percent on the second $250,000 guaranteed, and
- 3.875% on amounts above $500,000.

In addition, an on-going fee of 50 basis points (0.5 percent per annum) of the outstanding loan balance was mandated to be paid by the lender for the life of the loan.

In recent years, the cost of the 7(a) program has fallen due to improved underwriting and program improvements. However, reductions in federal funding for the program offset all of the cost reductions; none of the savings were used to reduce or rescind any of the 1994 fee increases.

NAGGL believes that borrowers should receive some benefits from an improving program and that it is time to begin reducing fees. Accordingly, we propose establishing a 1.25% subsidy rate floor. If program performance continues to improve or if for any other reason the subsidy rate would fall, SBA should be directed to begin reducing fees in order to maintain the subsidy rate at not less than 1.25%.

Historically, this Committee has agreed that 7(a) loans benefit much more than the borrower (for example, employment and the economy) and thus has advocated federal support or money in order to support the 7(a) loan program. This policy, however, has eroded over the past five years and could disappear completely in the next year or two. We urge that the Committee re-examine this matter and if you continue to agree that the Government should support small business lending, legislate a floor so that the entire cost of the program will not be imposed on borrowers.

H. R. 2615

Finally, I want to address related legislation which is pending before this Committee, H. R. 2615, which passed the House with overwhelming support last August. NAGGL strongly supports the provisions of this bill and urges the Committee to expeditiously hold hearings and consider it.

I have attached a summary of this legislation to my statement. I want to briefly mention one of its provisions: the imposition of pre-payment fees on borrowers with long term loans who make excessive prepayments in the first three years of the loan. These prepayments are increasing the cost of operating the 7(a) loan program due to the loss of anticipated fee income over the expected life of the loan. We have continued to advocate the imposition of a prepayment fee which would go solely to reduce 7(a) program costs as unless the anticipated fee income is replaced, subsidy rates will increase and thus necessitate the imposition of higher fees on future borrowers.

The 2001 budget request confirms that we are incurring higher costs on the program due to prepayments. Specifically, the subsidy rate includes an increase of 11 basis points primarily due to an increase in the loss of fee income due to loan prepayments and the loss of anticipated Treasury earnings on these fees.

We urge you to consider this issue carefully. As a matter of fairness, we believe that the cost burden caused by prepayments should be borne by those who choose to prepay their loans, not by future program users.

Thank you for the opportunity to comment. We look forward to working with you on this and related legislation during the remaining few months of this Congress.

NATIONAL ASSOCIATION OF GOVERNMENT GUARANTEED LENDERS

SUMMARY OF H. R. 2615

106th Congress

As Passed By The House August 2, 1999

Section 1. Levels of Participation

Increase the guarantee percentage on small loans of up to $150,000 (gross loan amount) to 80% (now 80% only up to $100,000).

Section 2. Loan Amounts

Increase the maximum amount of a 7(a) guaranteed loan from $750,000 to $1,000,000 (net loan); and establish a new gross loan maximum amount of $2,000,000 (guaranteed amount of the loan plus the unguaranteed amount).

Section 3. Interest on Defaulted Loans

Restore a lender's right to recover from SBA the full amount of interest accrued on a loan which goes into default and is liquidated.

Section 4. Prepayment of Loans

If a borrower voluntarily elects to make an excessive prepayment of the outstanding loan balance (i.e., more than 25% per year) within 3 years of disbursement of a loan which has an original term of 15 years or more, require him/her to pay to SBA a subsidy recoupment fee. The amount to be paid to SBA would be based upon the amount of the excessive prepayment:

- o 5% during the first year
- o 3% during the second year
- o 1% during the third year
- o zero thereafter.

Section 5. Guarantee Fees

Reduce the guarantee fee on small loans of up to $120,000 (net loan amount) to 2% (now 3% on the first $250,000).

Also, allow the lender to retain one-fourth of the 2% fee.

Section 6. Lease Terms

Allow a 7(a) borrower to lease-out not more than 20% of any property constructed with the proceeds of an SBA guaranteed loan. This is the same authority provided to 504 or Certified Development Company borrowers in 1997.

Document No. 48