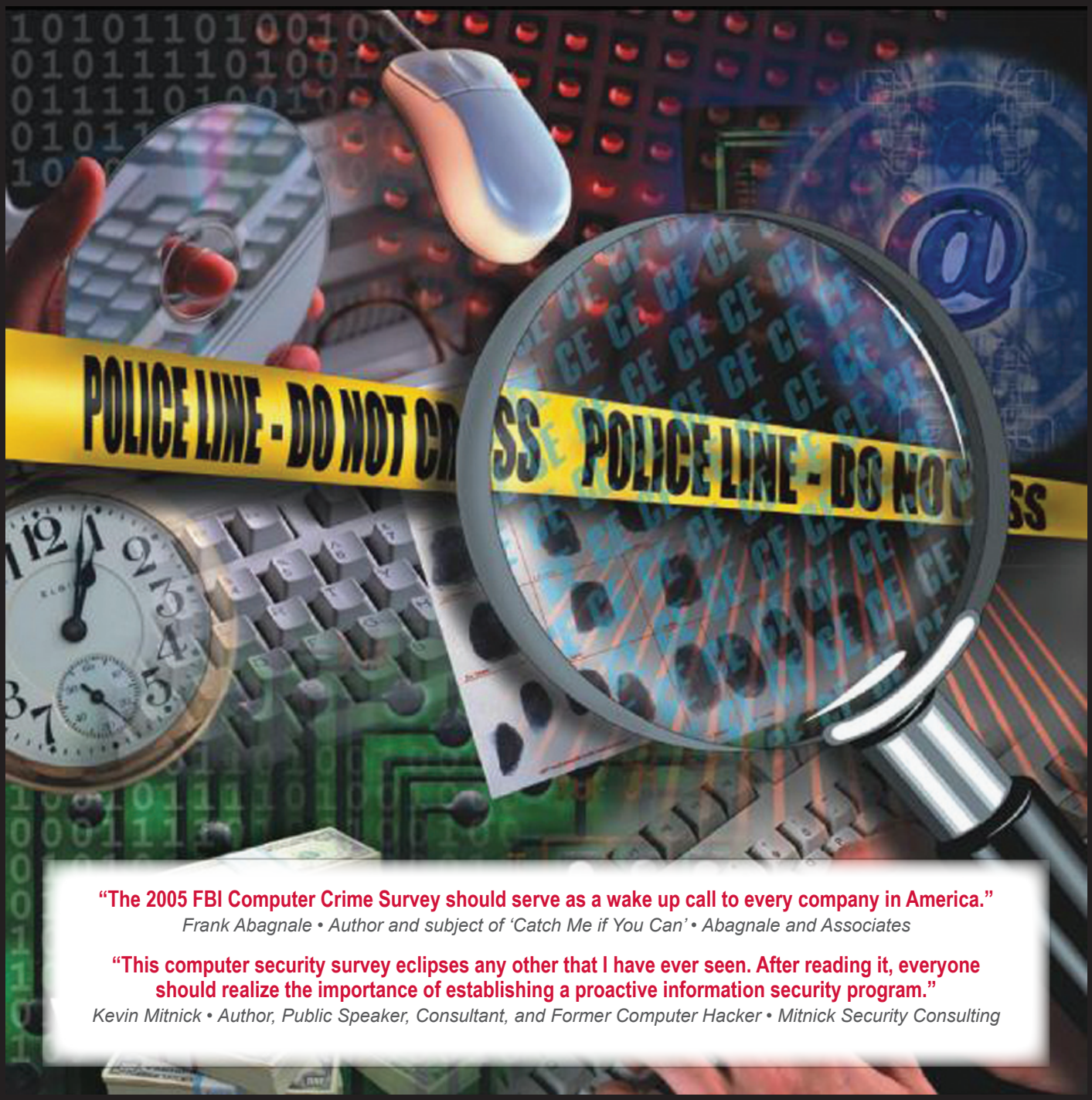
2005 FBI Computer Crime Survey



"The 2005 FBI Computer Crime Survey should serve as a wake up call to every company in America."
Frank Abagnale • Author and subject of 'Catch Me if You Can' • Abagnale and Associates

"This computer security survey eclipses any other that I have ever seen. After reading it, everyone should realize the importance of establishing a proactive information security program."
Kevin Mitnick • Author, Public Speaker, Consultant, and Former Computer Hacker • Mitnick Security Consulting

www.fbi.gov/publications/ccs2005.pdf

Table of Contents

Introduction 1
Key Findings 1
About the Questions 2
About the Recipients/Respondent 2
About the Methodology 2
Survey Results 3-15
About the Analysis 16
Using the Survey Statistics/Content 16
About the Contributors 17
Contact Information. 17

2005 FBI Computer Crime Survey

The 2005 FBI Computer Crime Survey addresses one of the highest priorities in the Federal Bureau of Investigation. These survey results are based on the responses of 2066 organizations. The purpose of this survey is to gain an accurate understanding of what computer security incidents are being experienced by the full spectrum of sizes and types of organizations within the United States. The 23-question survey addressed a wide variety of issues including: computer security technologies used, security incident types, and actions taken, as well as emerging technologies and trends such as wireless and biometrics. The survey was conducted in four states including Iowa, Nebraska, New York, and Texas and was performed by the corresponding FBI offices in those areas. The survey was conducted in such a way that recipients could respond anonymously.

This survey is not to be confused with the CSI/FBI Computer Crime and Security Survey, which has been conducted for several years, and has a somewhat different focus, method, and restricted number of respondents.

KEY FINDINGS:

- There are a variety of computer security technologies that organizations are increasingly investing in to combat the relentless, evolving, sophisticated threats, both internal and external. Despite these efforts, well over 5,000 computer security incidents were reported with 87% of respondents experiencing some type of incident.
- In many of the responding organizations, a common theme of frustration existed with the nonstop barrage of viruses, Trojans, worms, and spyware.
- Although the usage of antivirus, antispyware, firewalls, and antispam software is almost universal among the survey respondents, many computer security threats came from within the organizations.
- Of the intrusion attempts that appeared to have come from outside the organizations, the most common countries of origin appeared to be United States, China, Nigeria, Korea, Germany, Russia, and Romania.
- An overwhelming 91% of organizations that reported computer security incidents to law enforcement were satisfied with the response of law enforcement.
- Almost 90% of respondents were not familiar with the InfraGard (www.infragard.net) organization that is a joint effort by the FBI and industry to educate and share information related to threats to U.S. infrastructure.
- The survey respondents were very interested in being better informed on how to prevent computer crimes. Over 75% of respondents voiced a desire to attend an informational session hosted by their local FBI office.

DETAILED FINDINGS:

About the Questions:

The 2005 FBI Computer Crime Survey is unique in that the questions were compiled based on input from a large number and variety of organizations. Input for the questions was provided by both a large number of Special Agent computer intrusion investigators, supervisors, and Investigative Analysts within the FBI, as well as a variety of computer security professionals within the computer security and digital forensics communities. For the purposes of this survey, Computer Security Incident is defined as: Any real or suspected adverse event in relation to the security of computer systems or computer networks.

About the Recipients/Respondents:

Approximately 24,000 organizations received the 2005 FBI Computer Crime Survey. These recipients were from 430 different cities (with populations ranging from less than 1,000 to New York City, with a population of more than 8 million) from four states: Iowa, Nebraska, New York and Texas.

About The Methodology:

A letter was mailed to the recipients in mid June 2005. The following criteria were used to select the organizations which were provided by a list broker as well as other sources:

1. Organizations that had been in existence for three or more years.
2. Organizations that had five or more employees.
3. Organizations that fell within the geographic area requested (those 400+ cities covered by the FBI offices that participated).
4. Organizations that had $1,000,000 or more in annual revenue.

Organizations had to meet all four of these criteria in order to be selected. The letter was sent from the FBI and gave a brief description of the 2005 FBI Computer Crime Survey project. The letter conveyed the anonymous nature of the survey and directed recipients to a web address as well as provided a userid and password. Recipients had approximately five weeks to complete the survey. They were also given the option to request a written version although less than 1% did. 2066 individuals completed the survey. No reminders were sent.

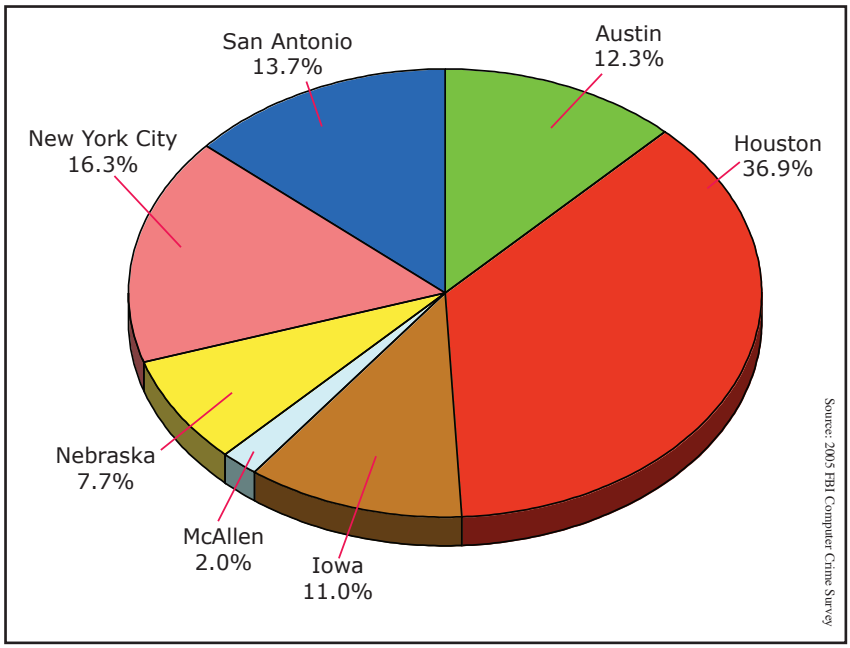
"The exponentially increasing volume of complaints received monthly at the IC3 have shown that cyber criminals have grown increasingly more sophisticated in their many methods of deception. This survey reflects the urgent need for expanded partnerships between the public and private sector entities to better identify and more effectively respond to incidents of cyber crime."

Daniel Larkin, FBI Unit Chief
Internet Crime Complaint Center (www.ic3.gov)

Question 1: In what general area is your organization located?

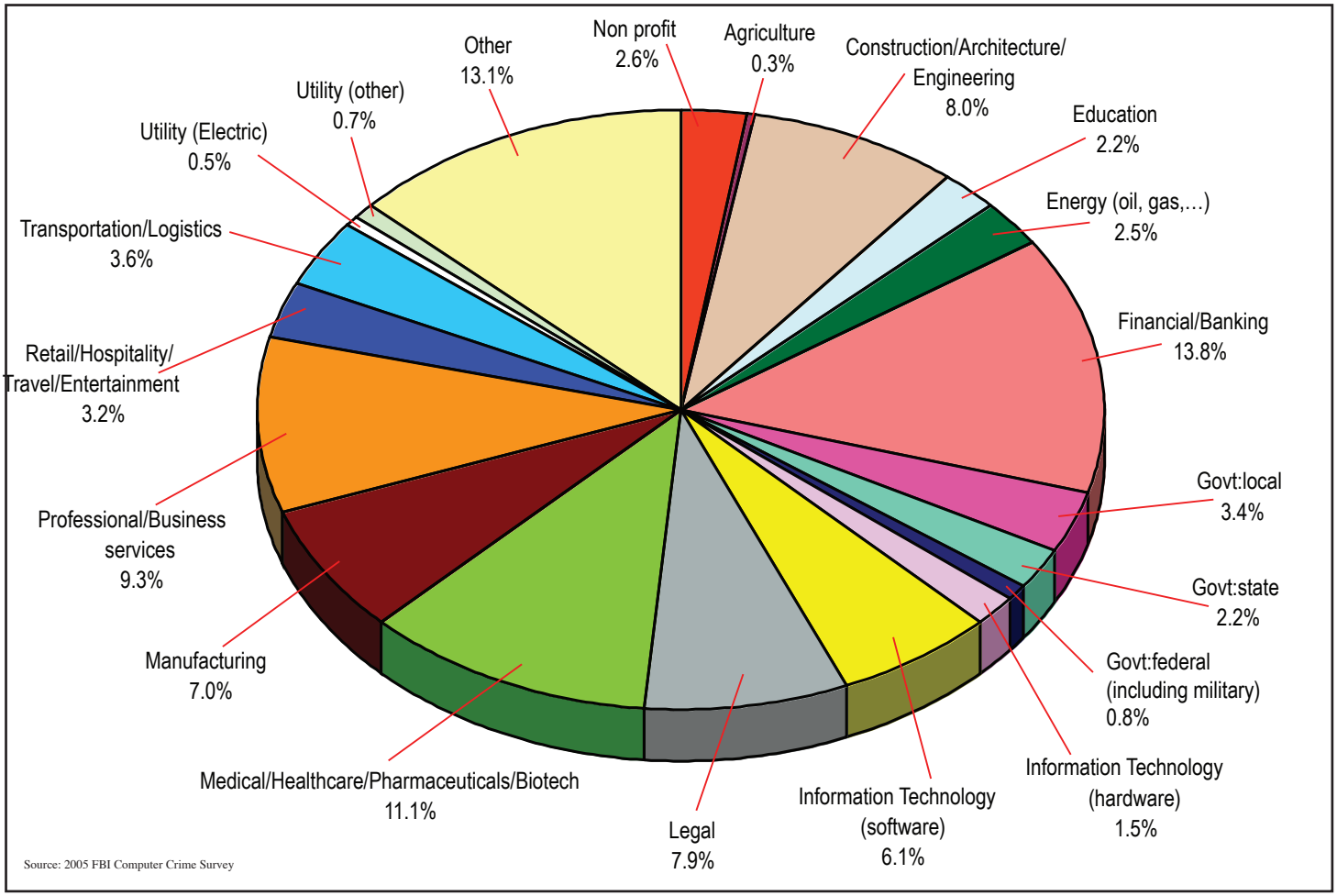
While responses from the survey came from several hundred different cities, there were a small number of primarily urban areas that made up the vast majority of respondents. Over 90% of the survey recipients were in the Austin, Houston, New York City, Iowa, Nebraska, and San Antonio metro areas. The Houston territory, which covers 40 counties, had the highest number of respondents with 762 while the Iowa/Nebraska territory had the highest percentage survey response with almost 13%.

2066 respondents



Question 2: What industry best describes your organization?

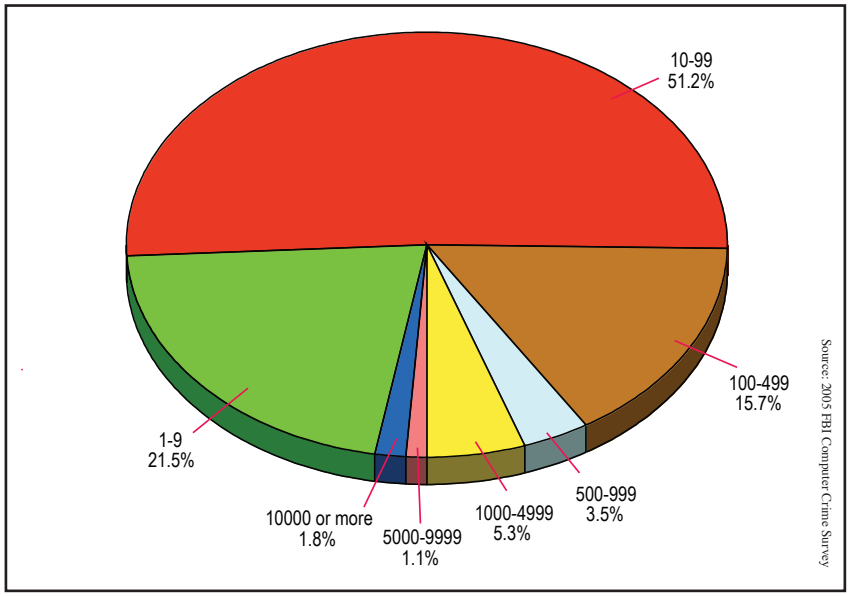
There are many ways in which organizations and businesses are categorized. Nineteen different categories were offered as well as an 'Other' category. While responses were received from every one of the categories, Financial (14%), Medical (11%), and Professional (9%) had the highest number of respondents. **2054** respondents



Question 3: How many employees does your organization have?

The survey respondents came from organizations from a broad size range from less than ten employees to well over 10,000 employees. The majority were, however, from with small to midsize organizations with over 51% coming from organizations from 10 – 99 employees.

2056 respondents

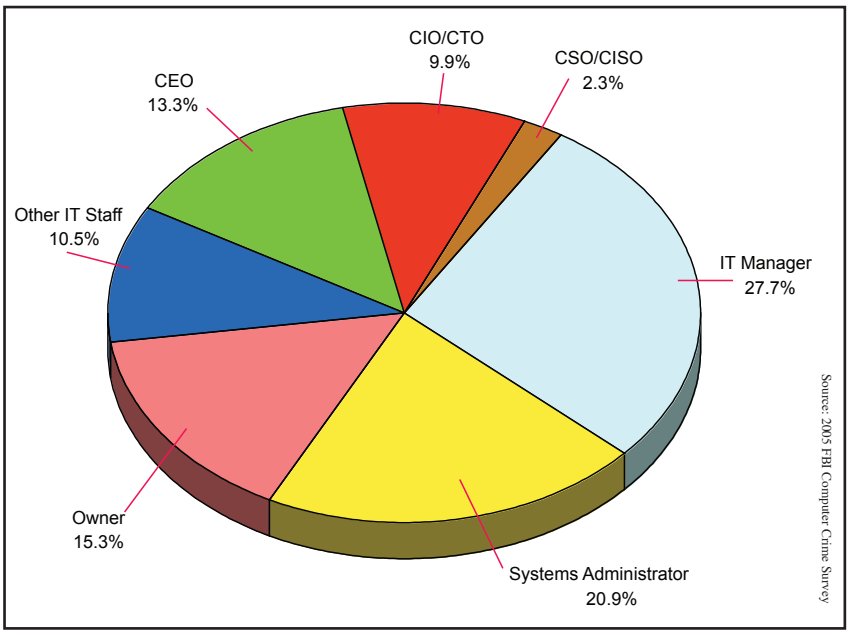


> **"Larger organizations are a bigger target for attackers, but they also have larger IT budgets and more standardization."**
>
> **Dr. Samuel Sander, Clemson University Computer Engineering Department**

Question 4: What best describes your title?

The job title of the respondents indicated that they were well qualified to answer the survey's questions. The largest group is 'IT Managers' (28%) with 'System Administrators' making up another 21%. Most small organizations would not have a Chief Security Officer or Chief Information Security Officer. This would account for only 2% of respondents indicating CSO/CISO instead of the more general IT related titles.

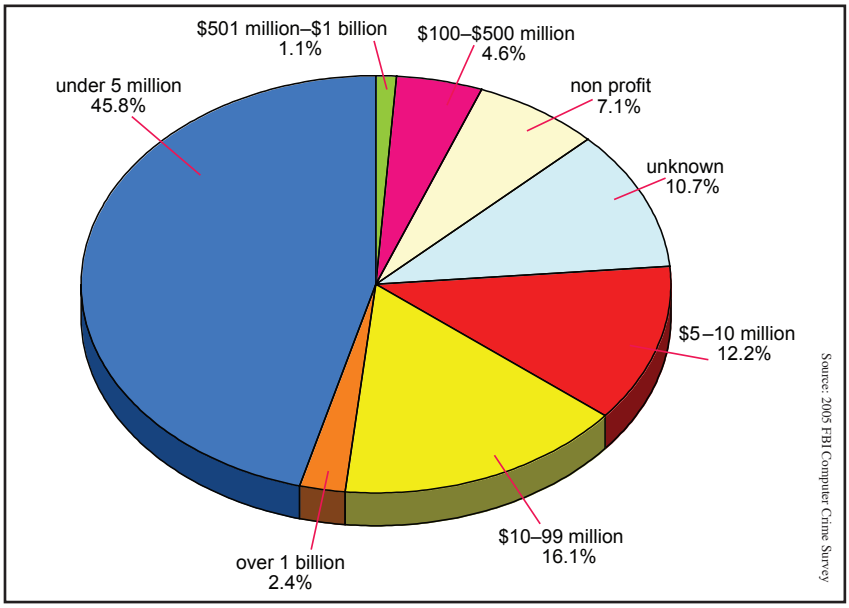
2040 respondents

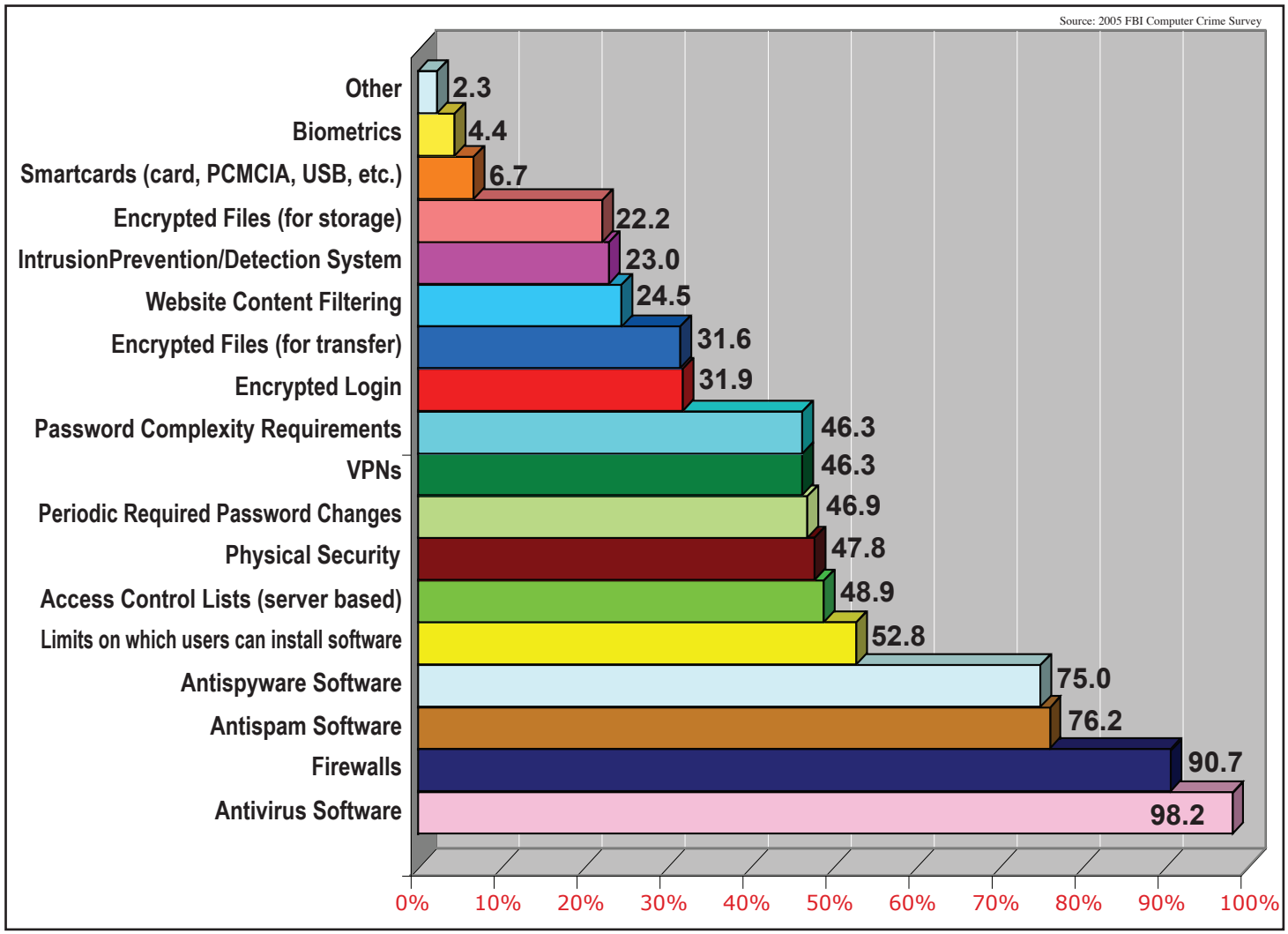


Question 5: What level of gross income does your organization have?

As expected, the largest gross income category by far was the 'Under $5,000,000' (46%) with the $10,000,000 - $99,000,000 category being a distant 2nd at 16%. Over 2% of respondents come from organizations with over a billion dollars of gross income.

2042 respondents





Question 6: Security technologies used by your organization:

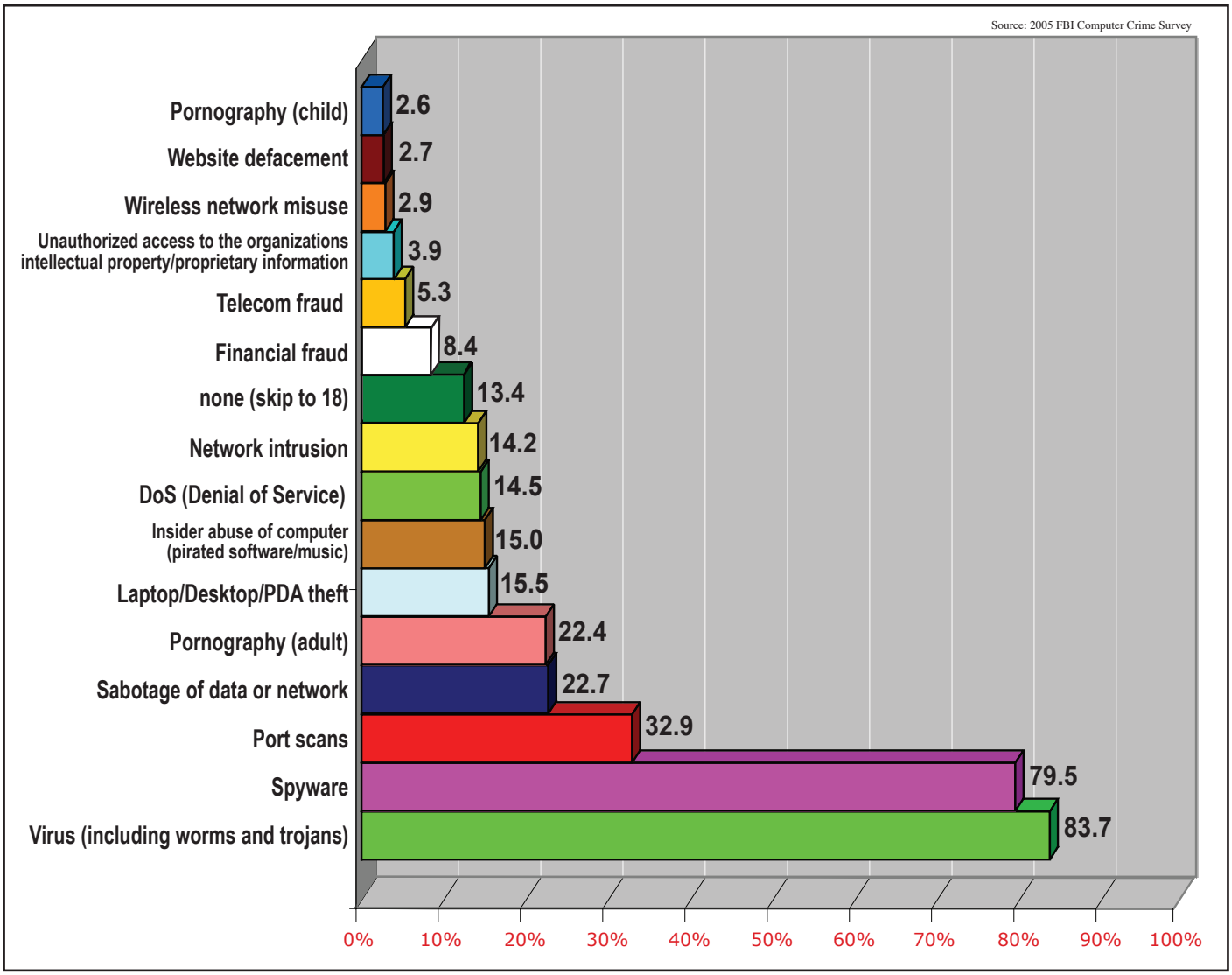
(select all that apply)

There was a large variety of security technologies being used among respondents. Usage of Antivirus software was almost universal with 98%. Firewalls were close behind with over 90% either using software or hardware firewalls. Operating system safeguards, such as limits on which users could install software, password complexity requirements, and periodic password changes were used by about half of respondents. Virtual Private Networks (VPNs) proved to be a popular means of achieving security with a 46% response. Advanced techniques such as biometrics (4%) and smartcards (7%) were implemented infrequently; however, it is anticipated that these numbers may increase in future surveys. Organizations used on average 7.8 of the security methods listed.

Interestingly, having more security measures did not mean a reduction in attacks. In fact there was a significantly positive correlation between the number of security measures employed and the number of Denial of Service (DoS) attacks. It is likely that organizations that are attractive targets of attacks are also most likely to both experience attack attempts and to employ more aggressive computer security measures. Also, organizations employing more technologies would likely be better able to be aware of computer security incidents aimed at their organizations. 2057 respondents

"…very few [organizations] use IDS and IPS solutions which can have a dynamic security environment."

Dr. Nimrod Kozlovski
Yale University, Computer Science Department, New York Law School
Author of 'The Computer and the Legal Process'



Question 7: Which types of computer security incidents has your organization detected within the last 12 months? (select all that apply)

Further analysis of the responses to this question indicate that the vast majority of respondents (87%) experienced some type of computer security incident. The average responding organization experienced several (2.75) different types of computer security incidents with each type potentially occurring multiple times (such as viruses and port scans) to an organization. Over 79% had been affected by spyware and not surprisingly almost 84% had been affected by a virus attack at least one time within the last 12 months, despite the almost universal usage of Antivirus software mentioned in the previous question. Port scans being at only 33% is a strong indicator that many respondents are not detecting the almost unavoidable port scans most networks experience. This may imply that even the 5,389 reported computer security incident types indicated by individual organizations may be significantly lower than the actual number. As expected, adult pornography was fairly high on the list of incident types at number five (395 responses) out of fifteen, with over 22% of organizations dealing with this issue. Although adult pornography is not illegal as child pornography is, it is against the policy of most organizations.

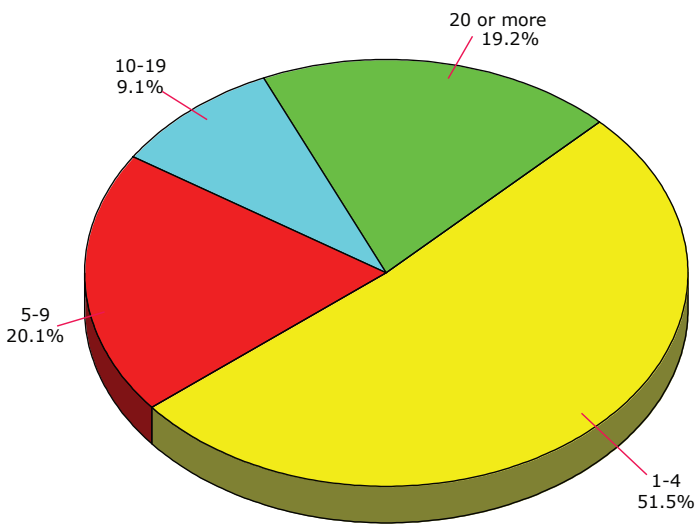
New York had the lowest percentage of organizations experiencing unauthorized access, but the highest percentage of experiencing insider abuse, laptop theft, telecom fraud, viruses, and website defacement. Austin, being the most high tech area surveyed, was home to the organizations most likely (over 91%) to have at least one type of computer security incident.

2039 respondents (**1762** respondents not including the 'None' responses)

Question 8: How many computer security incidents has your organization had within the last 12 months?

As indicated in the previous question's results, 87% of respondents experienced a computer security incident with only 277 implying that they did not have such an issue. Just over half of the responders to this question indicated that they had experience 1-4 incidents. Almost 20% of responses to this question indicated that they had experienced 20 or more such incidents. Large organizations (with gross income greater than one billion dollars) were more than twice as likely to be in the '20 or more attacks' category (45.5% of these larger organizations, compared to 19.2% of overall respondents). 40% of education and state government organizations had 20 or more incidents.

1787 respondents

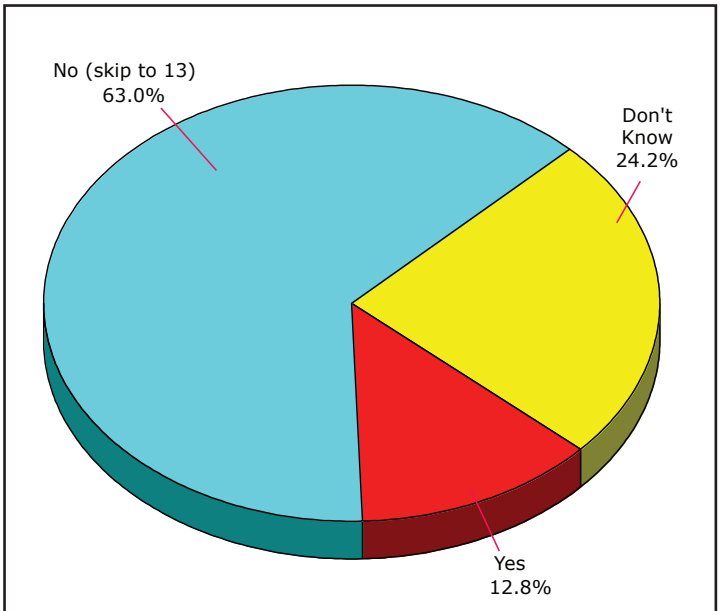


Source: 2005 FBI Computer Crime Survey

Question 9: Has your organization experienced unauthorized access to computer systems within the last 12 months?

The broad definition of 'computer security incident' (see the 'About the Questions' section) leads to a large number of victims in questions seven and eight. In question nine, the more restrictive category of organizations that experienced 'unauthorized access' to computer systems (this would not include viruses and port scans for example) is understandably smaller, but still significant. While an average of 13% knew that they experienced unauthorized access to their systems, 44% of educational, 31% of federal government, and 25% of transportation had experienced unauthorized access. An additional 24% stated that they did not know whether they had experienced such unauthorized access. This underscores the difficulty of organizations in having the expertise and resources to be aware of computer intrusions, much less guard against or prevent such breaches. 63% indicated that they had not had unauthorized access.

1811 respondents



Source: 2005 FBI Computer Crime Survey

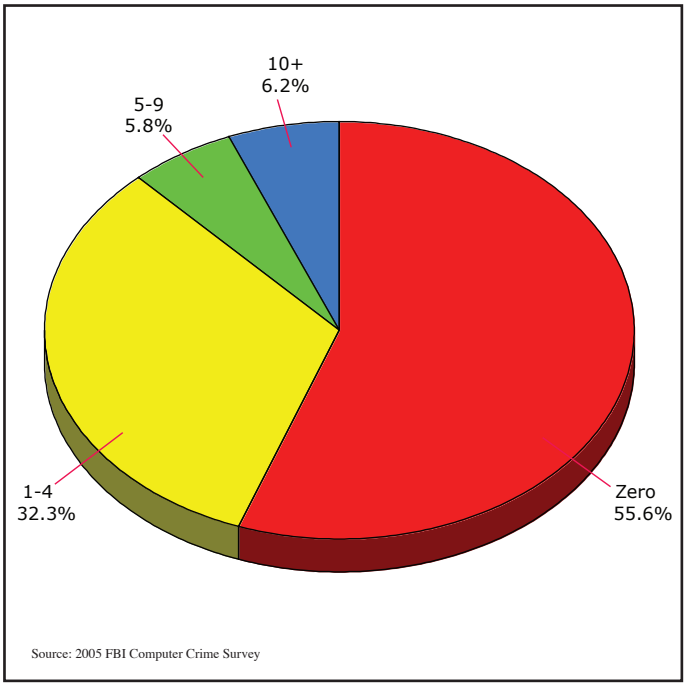
"It is likely that many of the organizations reporting an intrusion did not realize the duration, extent or severity of the intrusion, or detected only a portion of multiple separate intrusions during the reporting period."

Paul Williams
CEO, Gray Hat Research

Question 10: How many unauthorized access incidents were from within your organization?

Over 44% of respondents to this question had experienced intrusions from within their organization. This is a strong indicator that internal controls are extremely important and should not be under emphasized while concentrating efforts on deterring outside hackers. (It should be noted that some of the 232 respondents mentioned above could have been aware of computer security incidents originating from both within the organization as well as other such incidents originating outside the organization. Only respondents who answered 'Yes' to question 9 were tabulated for questions 10 and 11.)

226 respondents



"These results demonstrate the need for employee background checks on IT staff, as well as people in the mail room, accounts payable and accounts receivable."

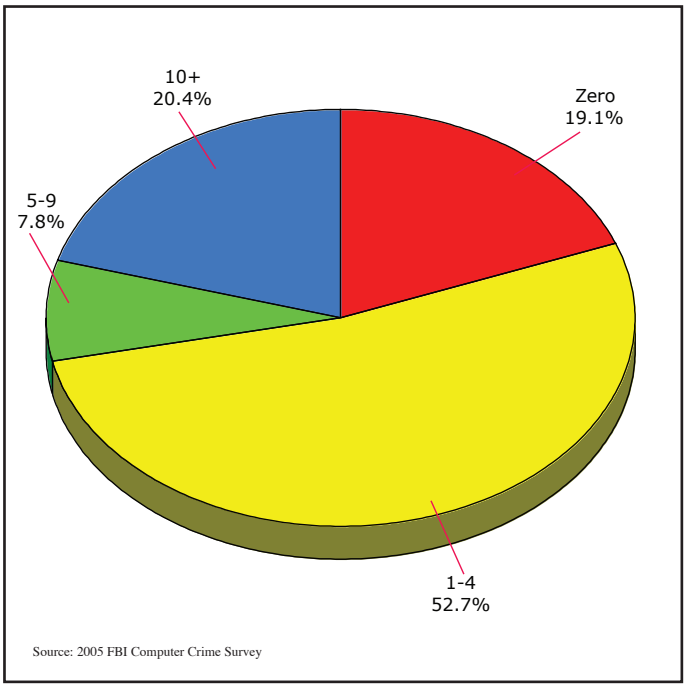
Frank Abagnale

Question 11: How many unauthorized access incidents were from outside your organization?

Overall, there were over twice as many unauthorized access incidents coming from outside the organization than there were from within, which underlines the importance of Intrusion Prevention/Detection Systems as well as firewalls, logs, password complexity, and other technology and physical security measures.

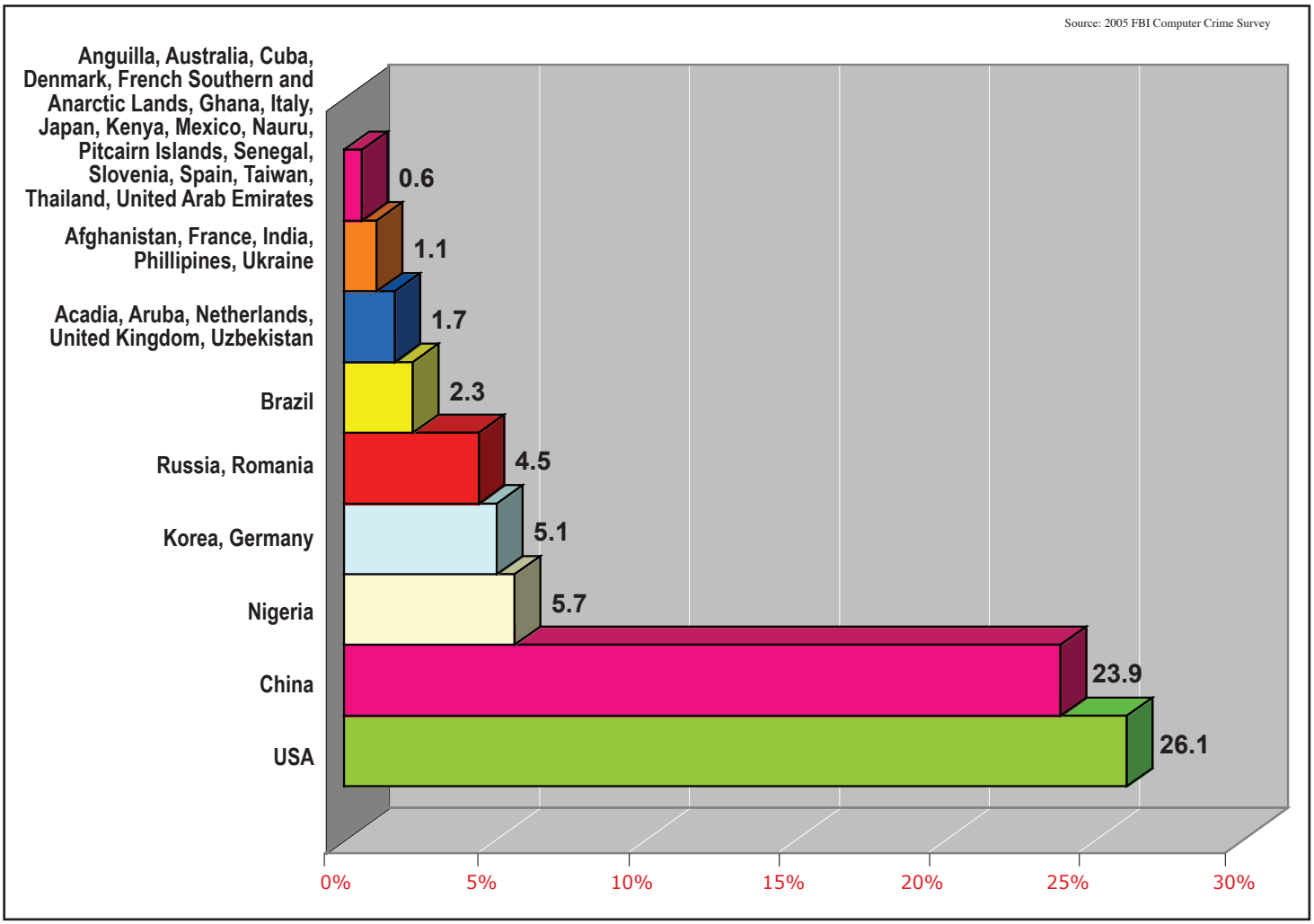
25% that said in question nine that they had experience unauthorized access believed that they had been intruded upon from both inside and outside their organization.

230 respondents



"I believe it is also relevant to note that the U.S. likely has the highest volume of Broadband home users as well as universities with Broadband high speed networks which are often unprotected, and as a result an attractive resource for cyber criminals."

Daniel Larkin



Question 12: What country was the most common source of the intrusion attempts against your organization?

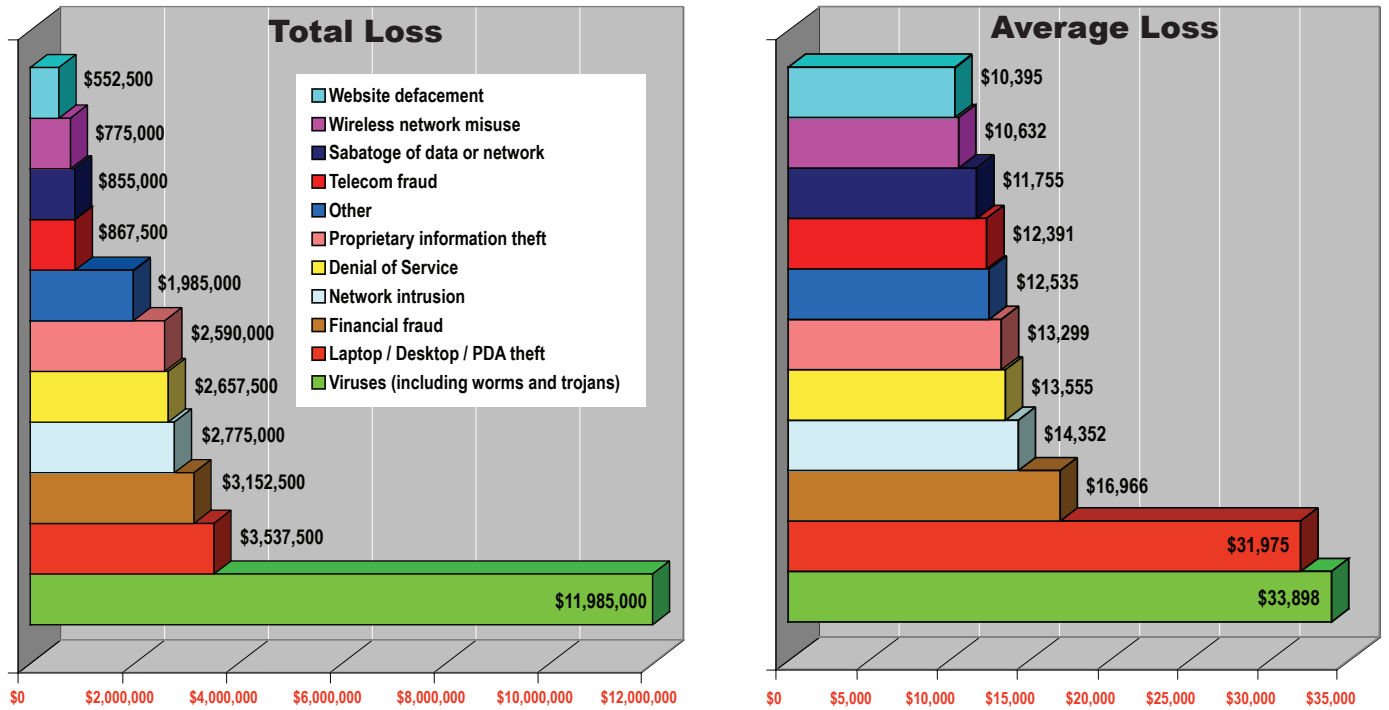
Question twelve drilled even deeper by trying to identify which countries were the most common source of the intrusion attempts. A surprising 53% of those organizations that had in the previous question identified an intrusion as coming from outside their organization also identified the country of origin. While 36 countries appear on the list, seven of the countries appeared to be the source for 75% of the intrusions. Two of the countries, USA and China, seem to be the source of over 50% of the intrusions. Difficulty tracking IP addresses and prosecution in China combined with other economic, military, and political concerns make this an unusually troubling statistic, especially when considering the potential impact of industrial espionage and state sponsored cyber warfare efforts. Organizations with higher revenue (greater than $5 million) were more than twice as likely to identify China as the source of the intrusion attempt. The number of positive responses to this question (176) is low enough that it is difficult to identify statistically significant trends with a high degree of probability.

Evidence of an intrusion that indicates a particular country may not be conclusive since computer hackers often use proxies and Trojanized computers in other countries to mask their identity and make detection difficult. An example of this type of stepping-stone attack would be a Romanian hacker that uses a proxy computer in China to access a compromised computer in the United States. This U.S. based computer would then be used to perform the computer intrusion. Those investigating the incident may falsely conclude that the source was within the United States.

176 respondents

> **"The major source of attacks are within the U.S. contrary to common myth…"**
> **Dr. Nimrod Kozlovski**

Question 13: What approximate dollar cost would you assign to the following types of incidents within the last 12 months? (business lost, consultant time, employee hours spent, ...)



Total approximate cost of security incidents for the organizations responding: $31,732,500
Note: Dollar figures were approximated by assuming that the average loss in each dollar cost range was the median value. For example, if a respondent indicated that the loss was between $5,000 and $15,000, a $10,000 loss was assumed. For the $100,000+ category, a $200,000 loss was used for the calculation.

Source: 2005 FBI Computer Crime Survey

While the vast majority of respondents were on the low end of each of the eleven categories as far as dollar loss, the financial impact is still very significant. The virus, worm, and Trojan category was over three times larger than any other category with almost $12,000,000 in losses. Simple laptop/PDA theft was the second highest category of financial loss with over $3,000,000.

In this question we can see that:

- 1324 (75.1%) of the 1762 organizations incurred a financial loss because of computer security incidents.
- This would indicate that 64.1% of the 2066 survey respondents incurred a financial loss.
- The average cost was over $24,000 each for the 1324 companies that indicated they did have a computer security incident.

Let's take a look at what the impact of computer intrusions might be in the entire U.S. as opposed to this sample of 2066 respondents. Conservative figures are intentionally used in the following extrapolation. While losses of approximately $32,000,000 are documented through this survey, the sample size is only one organization out of every 6292 across the U.S. (given an estimated 13,000,000 organizations). It is debatable whether 64.1% of the non-surveyed organizations would have experienced a financial loss from a computer security incident as is the case with those that responded. Some would argue that many of the organizations that responded did so because they had experienced a loss and were sensitized to the issue of computer security. Others might argue 64.1% is too low because as companies have been shown to be hesitant to report their crime, the same organizations would be hesitant to complete a computer crime survey in which they are asked about facts surrounding the intrusion.

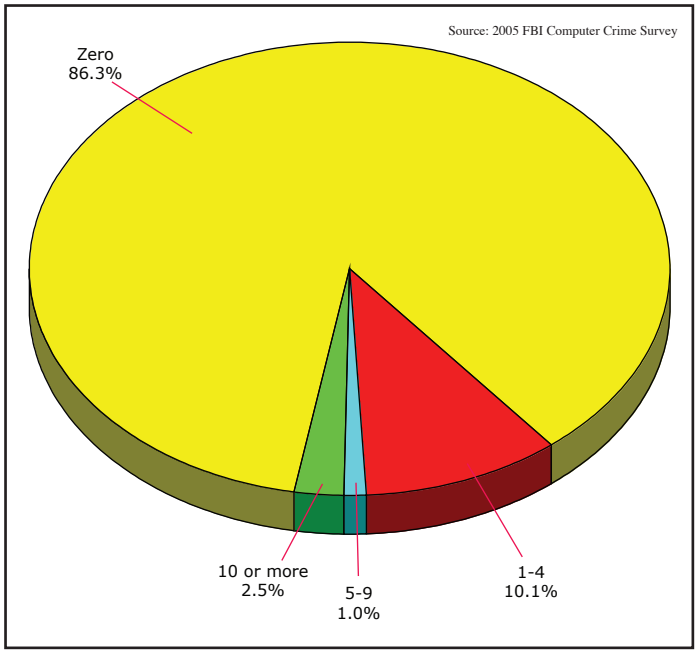
That being said, in an effort to be conservative, if the percentage of victims were 20% instead of 64.1% among those that did not receive a survey, this would be 2.8 million U.S. organizations experiencing at least one computer security incident with each of these 2.8 million organizations incurring a $24,000 average loss. This would total $67.2 billion per year or $7.6 million per hour. This figure is more than 1/2% of the entire U.S. Gross Domestic Product. While the loss figures are rough approximations, they are very conservative, assuming that non-survey respondents were only one third as likely to have experienced a financial loss. This clearly brings to light the high cost of computer crime to individual organizations and the economy as a whole. These figures did not include much of the staff, technology, time, and software employed to prevent such incidents. These figures also do not begin to address the losses of individuals who are victims of computer crime (intrusions, identity theft, etc.) or computer crime victims in other countries. 2066 respondents

"It appears that 'Proprietary information theft' is heavily under reported. Most organizations either have no way of even knowing if proprietary information was stolen from them and/or do not know how to quantify the loss." Paul Williams

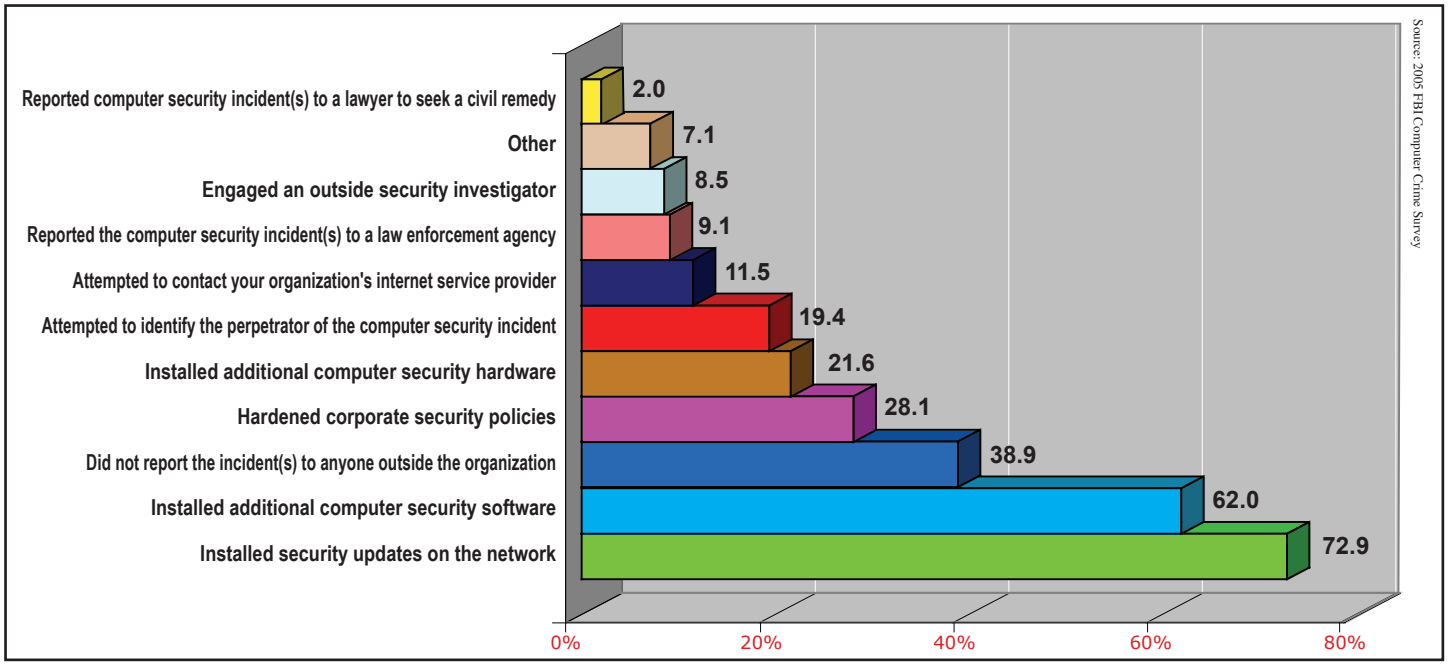
Question 14: How many website related security incidents occurred within the last 12 months on your organization's external website?

The vast majority of respondents (86%) had not experienced website related security incidents that they were aware of. About 14% of respondents experienced some type of website related security incident with the majority (74%) of those experiencing between one and four incidents. Over one quarter (26%) of those having issues in this area experienced five or more incidents and 2.5% of organizations had ten or more incidents.

1733 respondents



Question 15: If your organization has experienced a computer security incident within the last 12 months, which actions did your organization take? (select all that apply)



This question dealt with what actions were taken after a computer security incident. It produced several interesting observations. As one might expect, the top two responses were to install security updates and install additional computer security software. The next most common response of hardening corporate security policies could be an indicator that the incident originated within the organization and is also likely an indication that many organizations have corporate security policies that were not fully mature. Only (2%) of organizations chose to seek civil remedy through a lawyer.

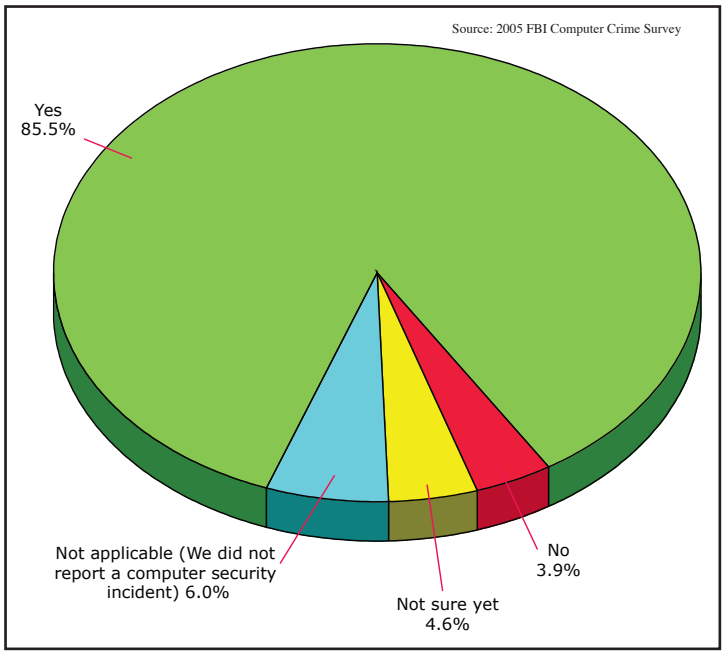
Although other computer crime surveys with a smaller number of respondents have indicated that approximately one in five victim organizations report the incident to law enforcement, the 134 that indicated in this survey that they had reported their incident to law enforcement indicates one in thirteen victims reporting to law enforcement. It should be noted that often, especially when incidents are small (port scans or minor previously known viruses for example), it may not be appropriate or necessary to contact law enforcement.

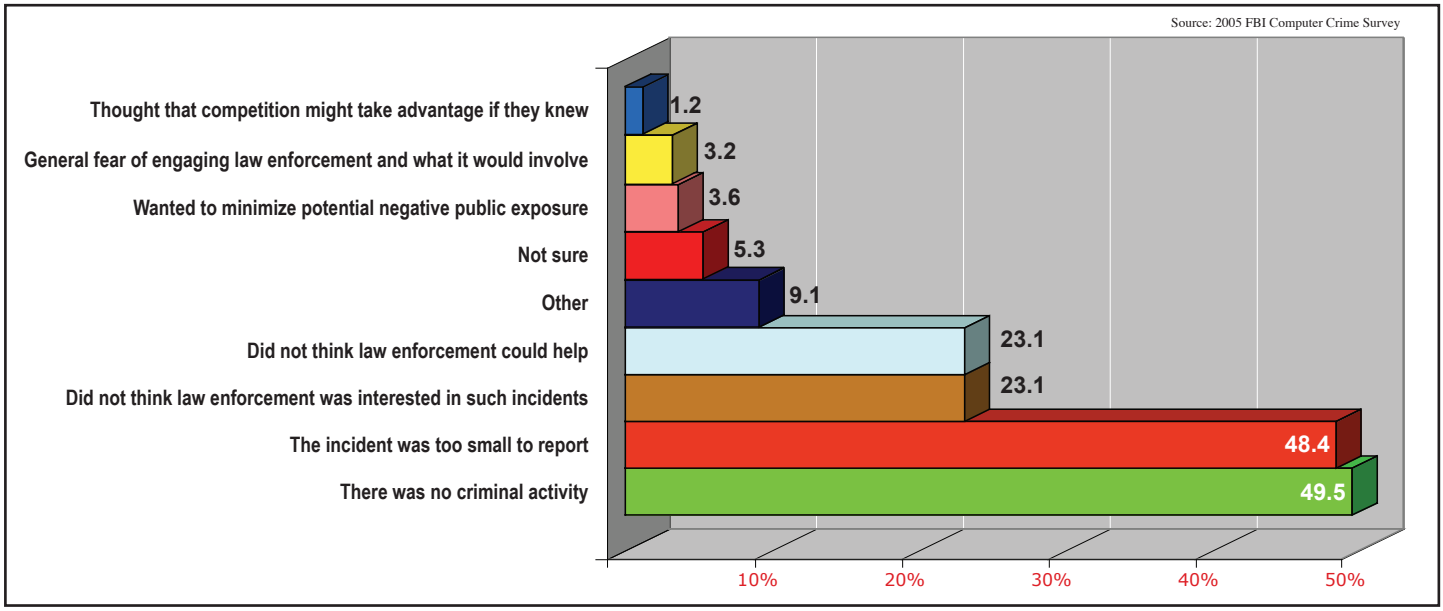
1467 respondents

Question 16: If your organization did report a computer security incident to a law enforcement agency, were you satisfied with the actions of that agency?

An overwhelming majority (91%) were satisfied with the actions of law enforcement. An additional 5% were not yet sure if they were satisfied, possibly due to ongoing investigation. Only 4% were not satisfied with law enforcements actions. This clearly addresses the concern of some organizations that law enforcement is either not equipped to investigate computer crime or is not interested in it.

1465 respondents





Question 17: If your organization did not report to a law enforcement agency, why did you choose not to? (select all that apply)

This question focused on those organizations that did not report to a law enforcement agency and the reasons for not doing so. As stated in question 15, we would expect that in a large number of incidents it would not be necessary to report to law enforcement. Just over 700 said there was no criminal activity and almost 700 indicated the incident was too small to report.

Those who thought law enforcement was not interested in such incidents numbered a disturbing 329 (23%). An equal number indicated they did not think that law enforcement *could* help. This may be due to the nature of the security incident or it may be the public's perception (or experience) that law enforcement was not equipped to investigate computer crime. While some individual law enforcement officers are not trained to respond to computer security incidents, local, state, and federal law enforcement agencies have become increasingly equipped to both investigate and assist in the prosecution of such violations. Computer related crime is the 3rd highest priority in the FBI, above public corruption, civil rights, organized crime, white collar crime, major theft and violent crime.

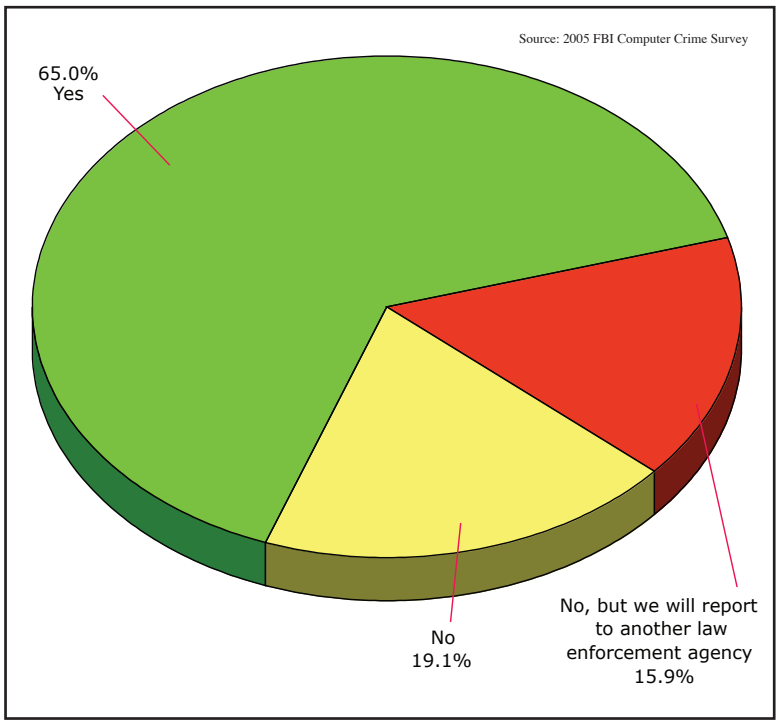
While law enforcement commonly hears about organizations' concern over minimizing public knowledge of a computer intrusion and concern over the effect on stock price for a public company, only 3% of respondents stated that minimizing potential negative public exposure was a reason for not reporting to law enforcement.

1423 respondents

Question 18: Will your organization likely report future cyber crime to the FBI?

In this question, we looked at future computer crime and asked whether organizations thought they would report future computer crime(s) to the FBI. Of the 1956 respondents, an encouraging 1272 (65%) indicated they would report an incident to the FBI, while an additional 16% stated that they would report to another law enforcement agency. The remaining 19% specified they would not report to law enforcement.

1956 respondents

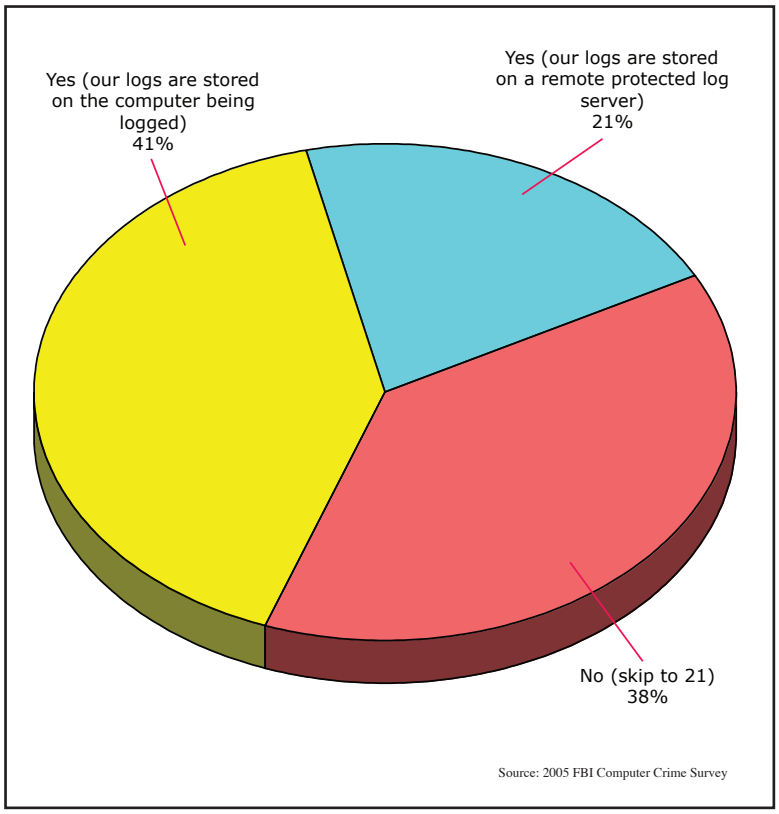


Question 19: Does your organization have computer security logging activated?

Logging of events on a computer network is a crucial element in tracking computer crimes. It is apparent that many organizations understand this important concept, as 62% had logging activated. Of those, 34% further secured their logs by storing them on a remote protected server. Unfortunately, there were 38% of respondents that did not have their logging capability activated. Federal government, legal, and manufacturing organizations were most likely to have logging activated. Surprisingly, utility companies were most likely to be unprotected in this area. The law enforcement community should look for opportunities to encourage organizations to enable logging.

Computer security consultant Kevin Mitnick had the following observations: "Organizations need to exercise more due diligence inspecting the audit logs. I've noticed a pattern of behavior in my security audits where some of my clients do not have the inclination or resources to examine these log files. We need to be vigilant in monitoring our networks rather than living under a false sense of security that these devices are going to manage themselves."

2018 respondents



"Almost 40% said they don't log for security purposes, and only 21% are storing logs on a machine other than the machine being logged. I'd imagine that this creates big gaps in the nation's ability to track security breaches back to their source. Industry, policy-makers and law enforcement should work together to make logging universal, secure, and affordable."

Dr. Simon Jackman, Stanford University, Department of Political Science and Department of Statistics

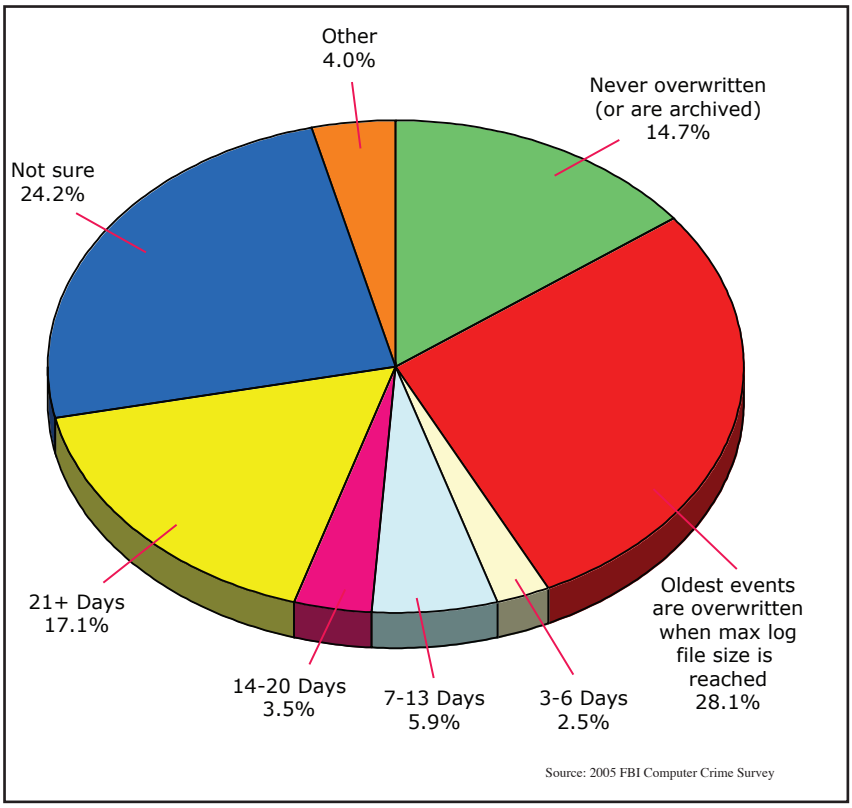
Question 20: How long are computer logs retained?

Of the respondents, only 15% gave the 'Never overwritten (or are archived)' answer that is optimal for investigations. The largest response of 356 (28%), overwrote their logs only when a maximum file size was reached. Depending on what that maximum file size is and how fast the log is filled, this strategy may or may not be sufficient. 12% of organizations only kept logs for three to twenty days, while approximately 17% kept logs for 21 or more days.

1269 respondents

"…the law must create incentives for better logging (and improved reporting as the California and New York law do)."

Dr. Nimrod Kozlovski

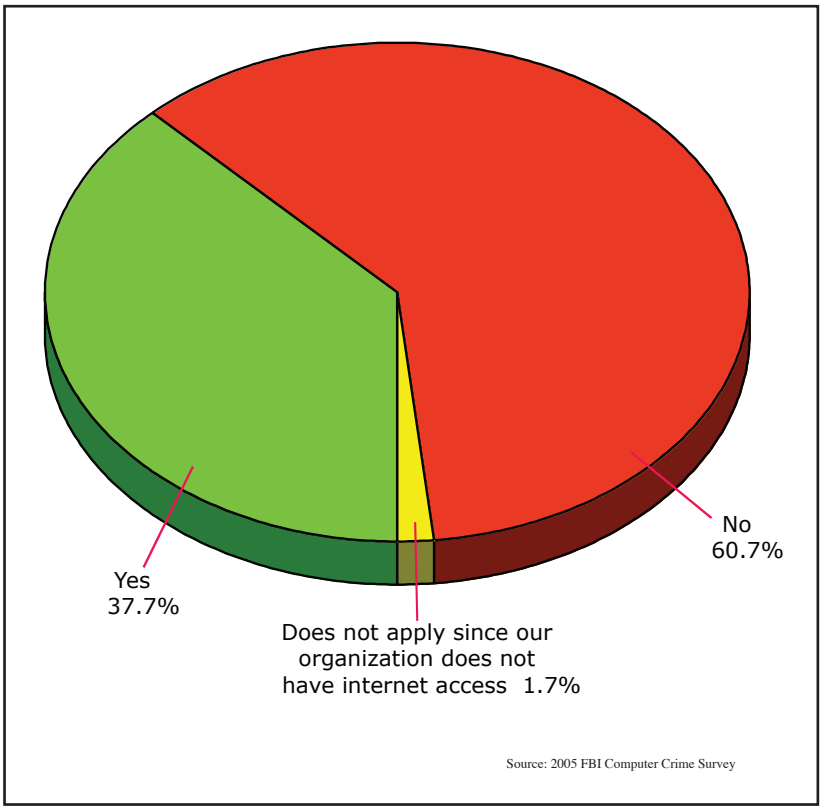


Question 21: Does your organization have website logging activated?

(for example: "Employee username" accessed "website X" at "date/time")

About 38% of respondents track the employee ID, website accessed, as well as the date and time. The majority of organizations, however, have no way of knowing what types of sites are being visited, how much time is being spent on the web, or which employees might be unnecessarily consuming needed bandwidth. Often simply making employees aware that this type of information is being logged will contribute to decreased non-business time on the internet and increased employee productivity. There have been several cases where an organization being able to pinpoint and stop an individual employees excessive music and video downloads significantly freed up desperately needed bandwidth.

1995 respondents

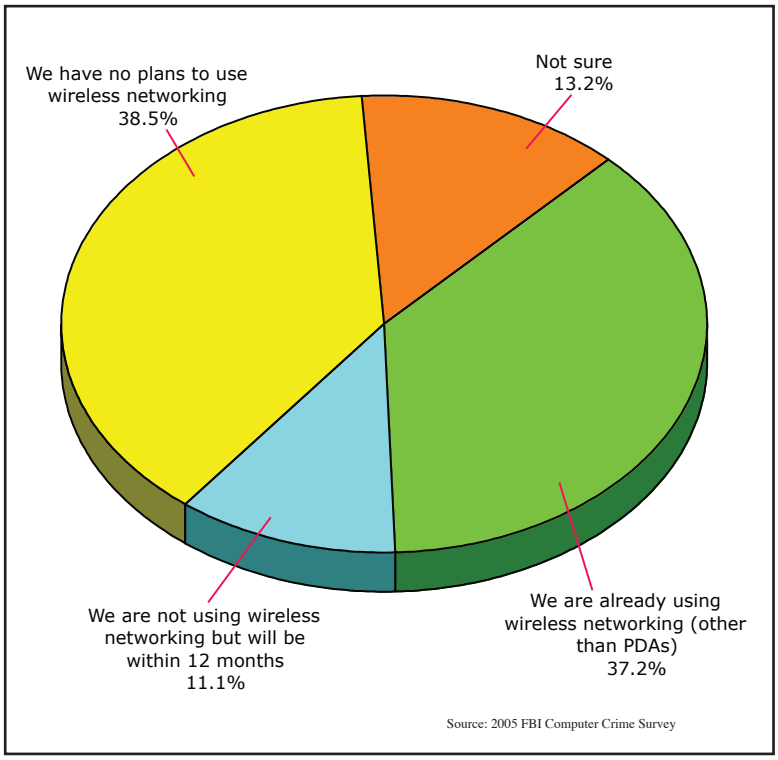


Question 22: What are your organization's plans in the area of wireless networking?

Over 37% of respondents are already using wireless with an additional 11% planning to implement wireless within the next 12 months. A large group, 786 (38%), had no plans to implement wireless technology. The remaining 13% were undecided. Education, IT, agriculture, and electric utilities were 70% or more likely to be using or planning to use wireless technology.

Computer security consultant Kevin Mitnick comments: "With the rush to enjoy the benefits of wireless connectivity, countless wireless access points are deployed with no security. In other cases, the administrator may enable WEP (Wired Equivalency Privacy) on these devices in an effort to protect their networks. Unfortunately, cracking a WEP key is like taking candy from a baby. Organizations need to clearly understand the risks and benefits of using such technology, and investigate what configurations will provide them the desired level of security appropriate for their environment."

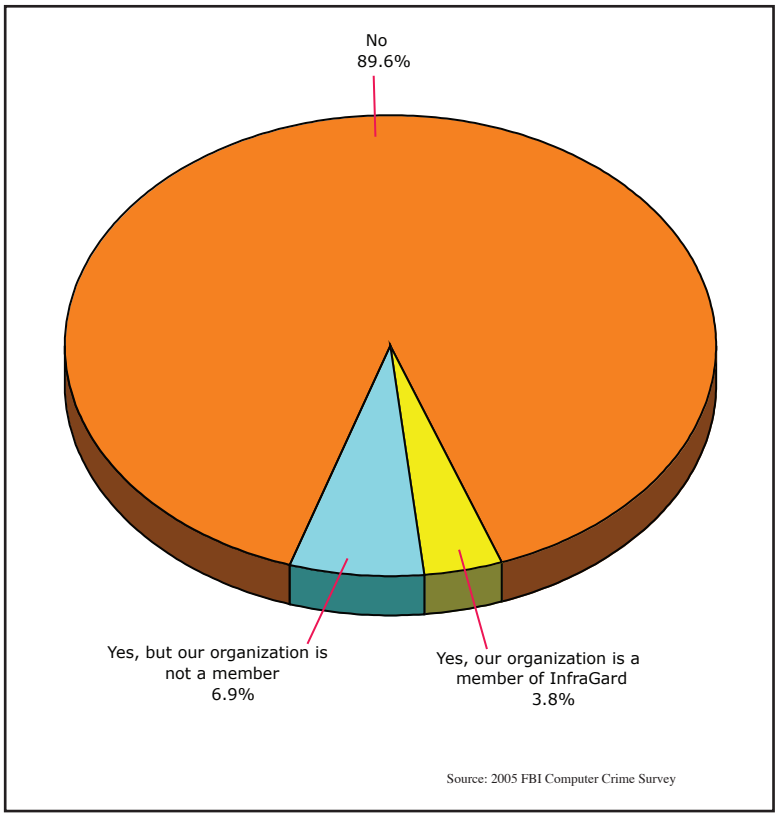
2043 respondents



Question 23: Are you familiar with the InfraGard organization?

InfraGard has as its mission to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures. Only 11% of respondents were familiar with the organization including 4% that were currently InfraGard members. The vast majority, almost 90%, was not familiar with InfraGard, although most have a local chapter in their area. While a small percentage of survey recipients are not located near an InfraGard chapter, the vast majority of respondents do have a chapter in their area. For additional information see www.infragard.net.

2051 respondents



"The threat of confidential information being stolen by an employee or an outsider is no longer a question of 'if,' but of 'when.' Every company, both large and small, should study this survey and use the data as the basis for making changes. Those who ignore it do so at their peril."

Frank Abagnale

"I continue to be surprised - not at the variety of incidents - but at the magnitude of flaws in deployed systems and the subsequent attacks and losses, all of which are accepted as "business as usual." As the Presidents Information Advisory Committee (PITAC, URL below) noted in our February report, there is a crisis in cybersecurity. So long as we continue to apply patches and spot defenses to existing problems, the overall situation will continue to deteriorate. Without a significant increase in focus and funding for both long-term cyber security research and more effective law enforcement we can only expect more incidents and greater losses, year after year."

Dr. Eugene Spafford
Purdue University, Computer Security Professor, Advisor to Presidents Bill Clinton and George W. Bush
Director of the Center for Education and Research in Information Assurance and Security(CERIAS)
PITAC report: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

About the Analysis:

The analysis of the survey results was compiled after assimilating the input of a large number of experts in a variety of fields including statistics, computer science, computer crime investigation, digital forensics, law enforcement, and journalism. Seven PhD university professors from Clemson, Purdue, Stanford, West Point, UC Berkeley, and others, as well as analysts from the Internet Crime Complaint Center (www.IC3.gov), and the FBI also helped refine the resulting analysis. In addition, many experts from the computer security industry offered insightful input. The percentage values have been rounded to the nearest integer in the analysis portion. The percentages found in the graphs have been rounded to the nearest 1/10th% causing the totals for some of the questions to not be exactly 100%.

Using The Survey Statistics/Content:

We strongly encourage use of the information and statistics found in this survey if used properly. All use must strictly comply with the following:

1. You must state that the material comes from the 2005 FBI Computer Crime Survey.
2. For any broadly distributed (beyond 100 recipients) or published work, you must send a copy of the work to the contact at the end of the survey, or if online, the website address of the work. If the information was used in another way, such as a verbal presentation, you must state how it was used in an email or letter to the contact at the end of this survey.
3. You may not profit directly from the use of the information contained in this survey. You may however use the information as a small part of a presentation, book, or other similar works.

Again, we encourage use and distribution of the survey information.

About The Contributors:

There were many that contributed to both the survey questions and the analysis.

The major contributors are (in alphabetical order):

Frank Abagnale – Abagnale and Associates
Author of 'Catch Me if You Can', Lecturer, Consultant, National Cyber Security Alliance spokesman

Prof. Matt Bishop – University of California Davis
Computer Security Professor, Author of 'Computer Security: Art and Science'

LTC Dr. Andrew Glen – United States Military Academy
Associate Professor, Department of Mathematical Sciences

Dr. Simon Jackman – Stanford University
Political Science and Statistics Professor

Dr. Nimrod Kozlovski – Yale University,
Computer Science Department, Adjunct Professor of Law at New York Law School,
Author of 'The Computer and the Legal Process'

Daniel Larkin – Internet Crime Complaint Center
(www.IC3.gov); FBI Unit Chief

Kevin Mitnick – Mitnick Security Consulting
Author, Public Speaker, Consultant, and Former Computer Hacker

Dr. Tom Piazza – University of California Berkeley
Senior Sampling Statistician, Survey Research Center

Dr. Sam Sander – Clemson University
Computer Engineering Professor

Dr. Eugene Spafford – Purdue University
Computer Security Professor, CISSP, ISSA Hall of Fame,
security advisor to Presidents Bill Clinton and George W Bush

Bruce Verduyn – FBI
Special Agent, Cyber Squad

Paul Williams – Gray Hat Research
Chief Technology Officer, MCSE, NSA IAM and IEM

Ray Yepes – Computer Security Consultant
CISSP, MCSE, MCP, NSA IAM and IEM, Homeland Security level 5, CCNP, CCSP

Opinions found in this report are those of one or more of the contributors and not necessarily those of the Federal Bureau of Investigation.

This report can be found online at: www.fbi.gov/publications/ccs2005.pdf

Contact Information:

Special Agent Bruce Verduyn
Houston FBI – Cyber Squad
2500 E TC Jester Blvd
Houston, TX 77008
bruce.verduyn@ic.fbi.gov
713-693-5000