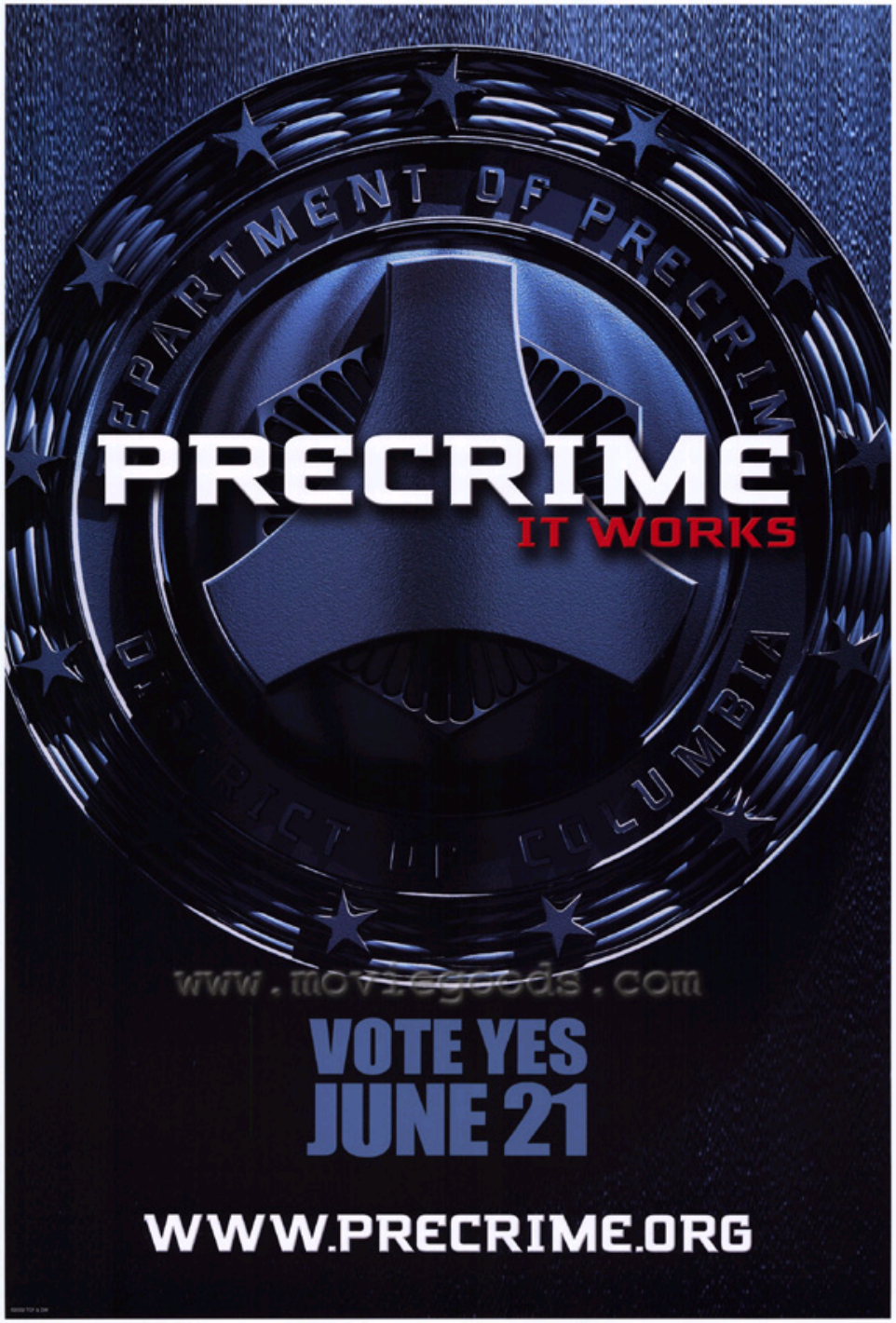
Section 2: Cybercrime


DEPARTMENT OF PRECRIME
DISTRICT OF COLUMBIA
PRECRIME
IT WORKS
www.moviegoods.com
VOTE YES
JUNE 21
WWW.PRECRIME.ORG

Lecture Outline

1. Crime in the Digital Age
    a. How much crime
    b. Types of Computer crime
2. White Collar Crime
    a. Embezzlement
    b. Corporate Espionage
    c. Money Laundering
    d. Counterfiting
    e. Identity Theft

"Cybercrime"

How much cybercrime is there?

Numbers for victims and the extent of the damage to victims is virtually impossible to determine.

However there are numbers that are often reported that give us a view of the extent of the damage

- 828 million in fraudulent VISA transactions in 1997
- RIAA claims to have lost billions to Napster alone
- Hundreds of thousands of victims are cyberstalked.
    - Approximately 1 in 12 women is stalked some time during their life, increasingly using the Internet.
- Majority of all businesses are victims of some type of computer crime.

"Cybercrime"

Nature and extent of cybercrime

Hard numbers are difficult to come by because of the nature of the crime and because there is not a standardized collection process.

- Government doesn't keep records
- Victims don't know they have been victims
- Many corporations don't want to report victimizations

Some of the best data comes from a survey conducted by the Computer Security Institute (CSI) and the FBI

Survey of 503 security practioners who work for major corporations or large government agencies.

Cybercrime

Nature and extent of cybercrime

Results of survey

- 90% of respondents detected security breaches within the last 12 months.
- 80% reported financial loses due to computer breaches.
  - Losses from 223 respondents totaled $455,848,000 in 2001.
  - Information theft resulted in 170,827,000 in loses.
  - Financial fraud resulted in $115,753,000 in loses.
- 74% cited the internet as the most frequent point of attack.
- Only 34% of crimes were reported to law enforcement

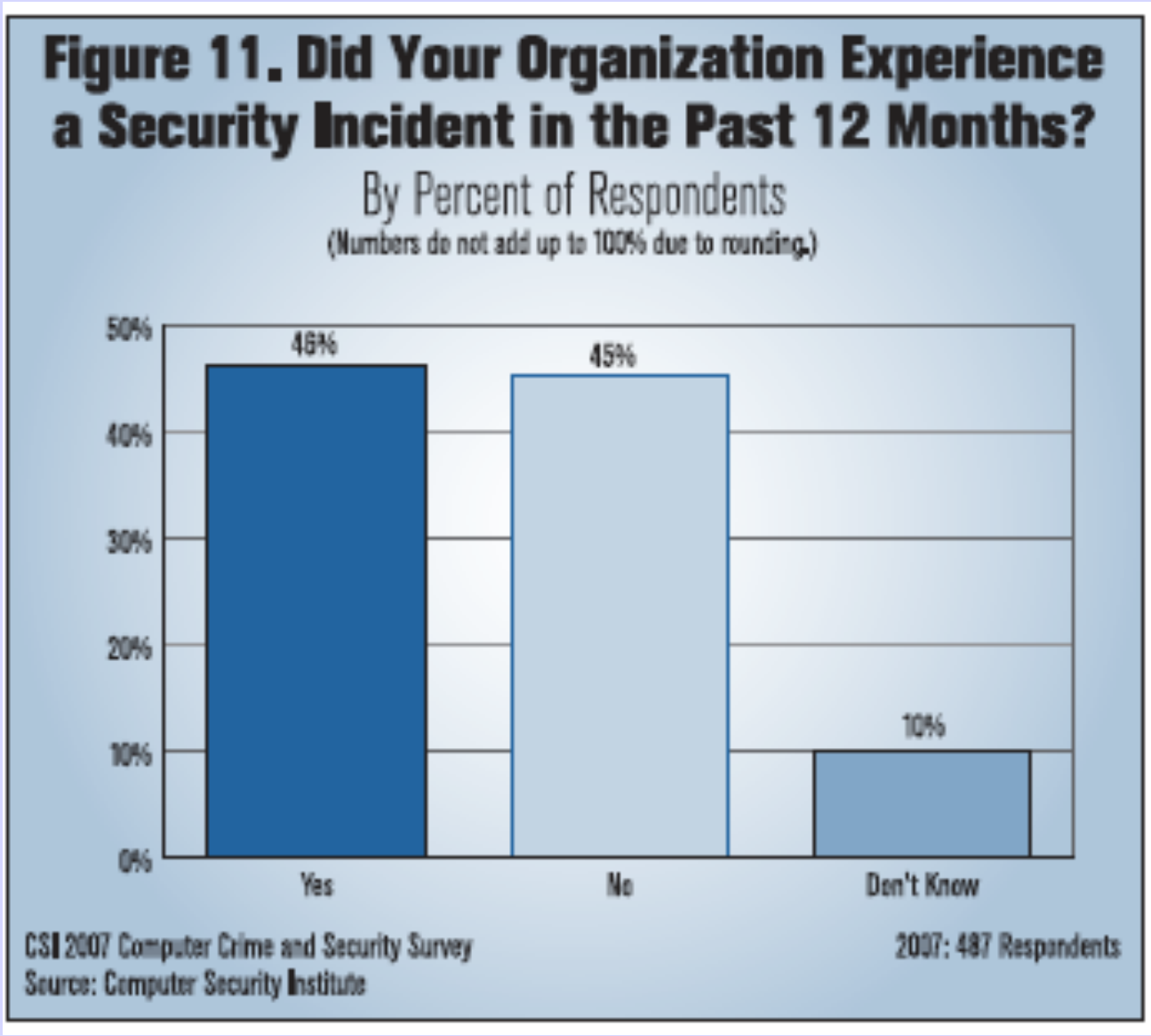


Figure 11. Did Your Organization Experience a Security Incident in the Past 12 Months?
By Percent of Respondents
(Numbers do not add up to 100% due to rounding.)
50%
40%
30%
20%
10%
0%
46%
45%
10%
Yes
No
Don't Know
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 487 Respondents

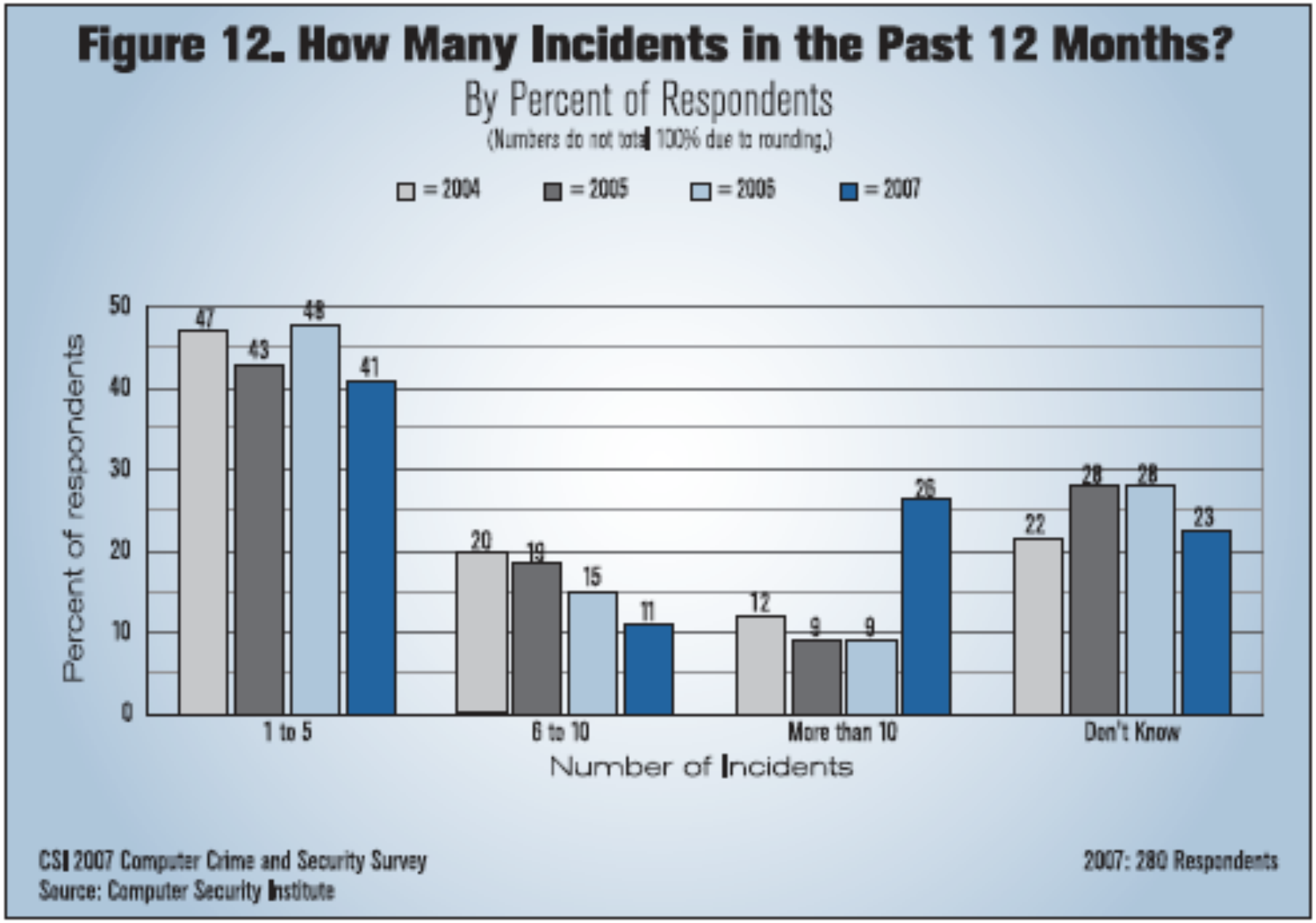


Figure 12. How Many Incidents in the Past 12 Months?
By Percent of Respondents
(Numbers do not total 100% due to rounding.)
= 2004
= 2005
= 2006
= 2007
Percent of respondents
50
40
30
20
10
0
47
43
48
41
20
19
15
11
12
9
9
26
22
28
28
23
1 to 5
6 to 10
More than 10
Don't Know
Number of Incidents
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 280 Respondents

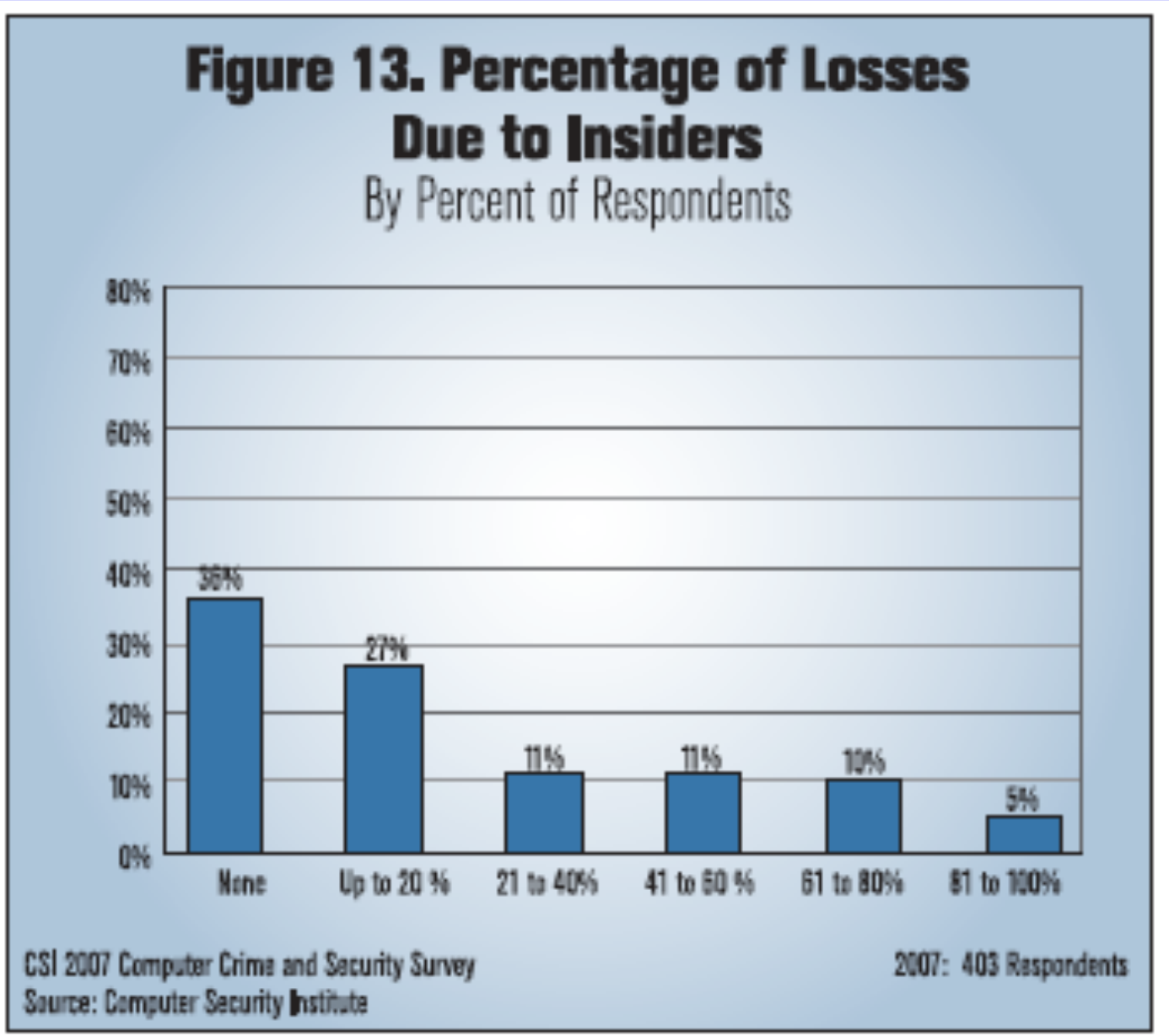
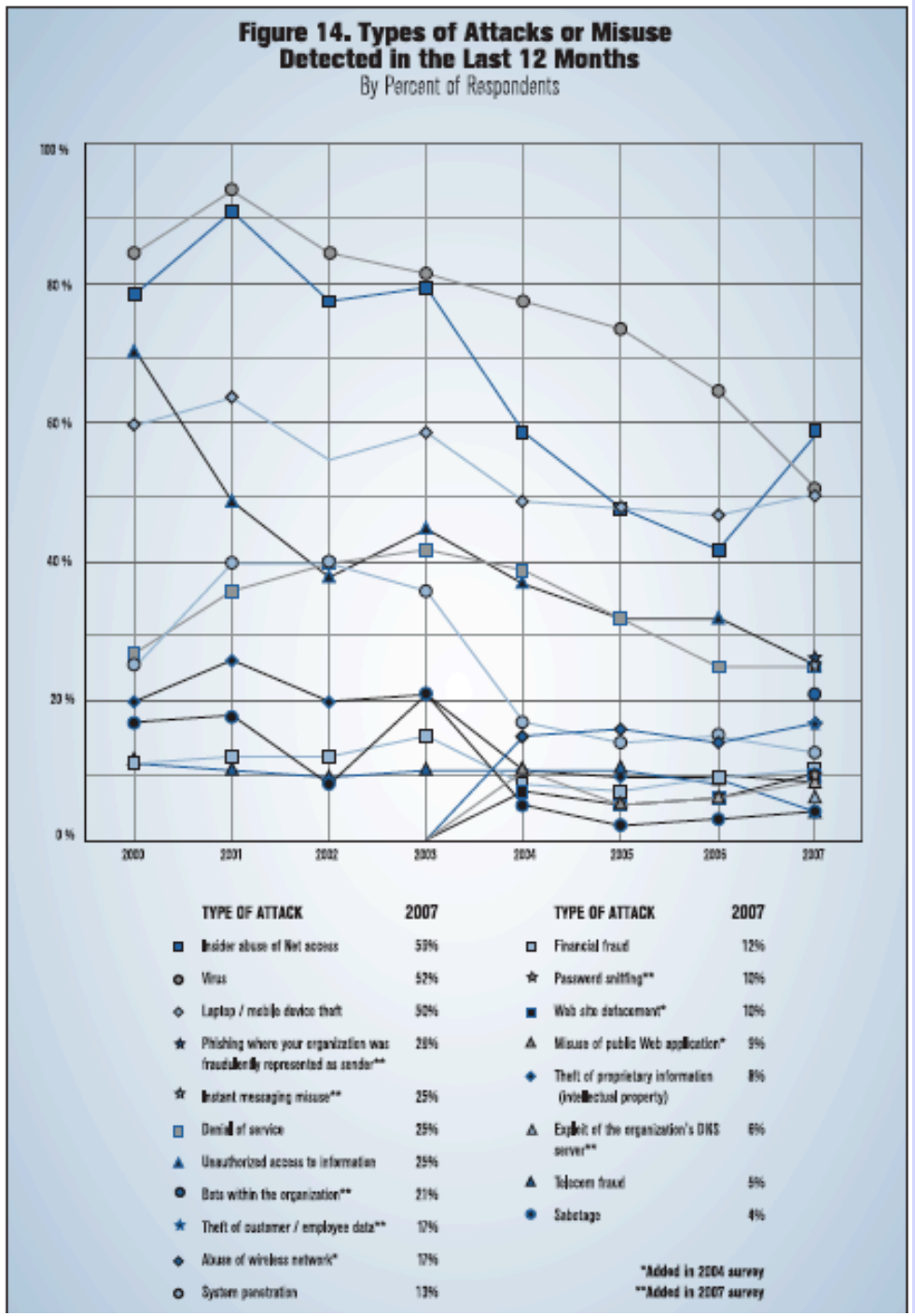
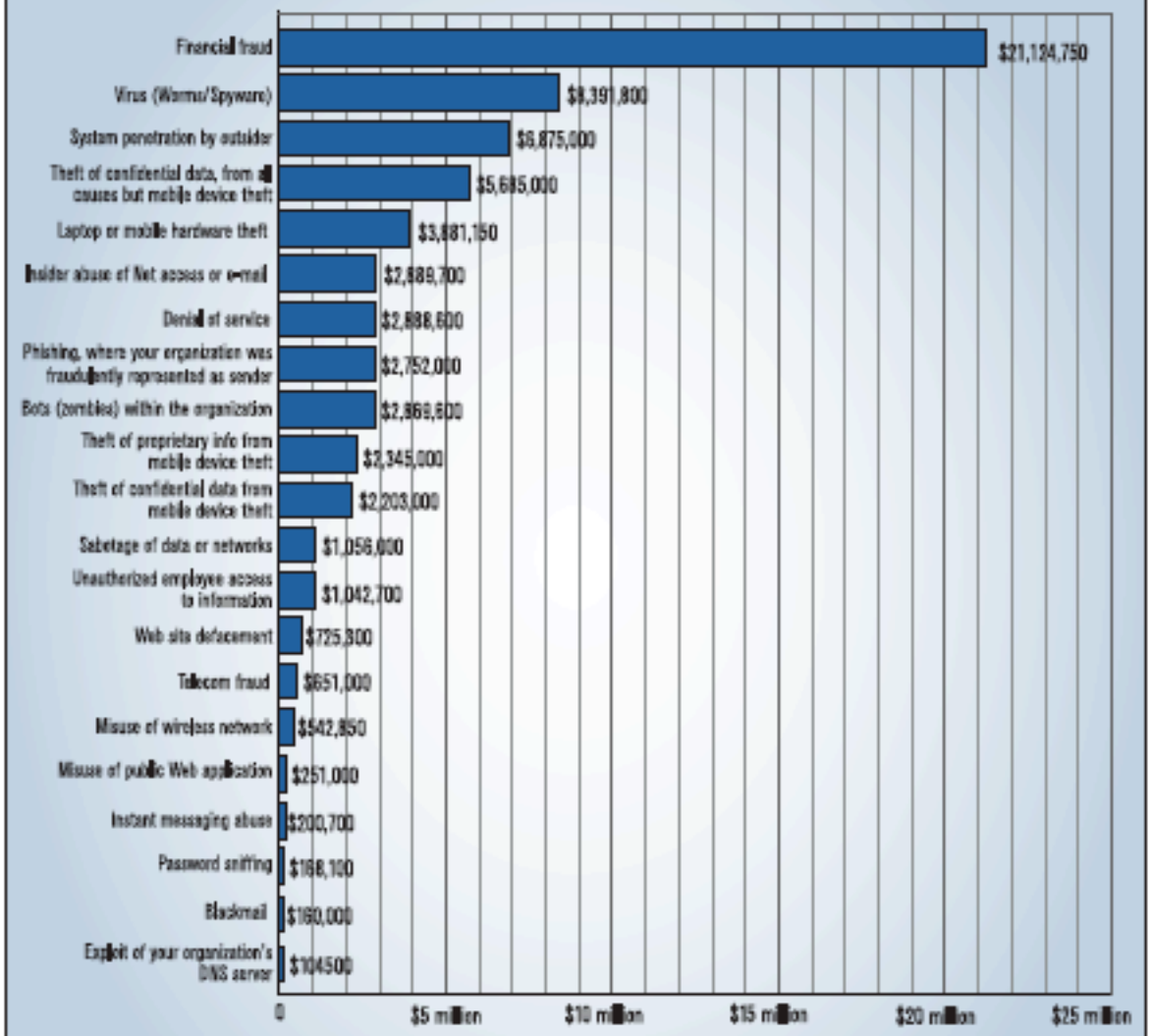


Figure 13. Percentage of Losses Due to Insiders
By Percent of Respondents
80%
70%
60%
50%
40%
30%
20%
10%
0%
36%
27%
11%
11%
10%
5%
None
Up to 20 %
21 to 40%
41 to 60 %
61 to 80%
81 to 100%
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 403 Respondents



1. Insider abuse of net access
2. Virus
3. Laptop/mobile device theft
4. Phishing
5. Instant messaging misuse

Figure 16. Dollar Amount Losses by Type of Attack



Total Losses for 2007 = $66,930,950

(Numbers above do not equal total due to rounding.)

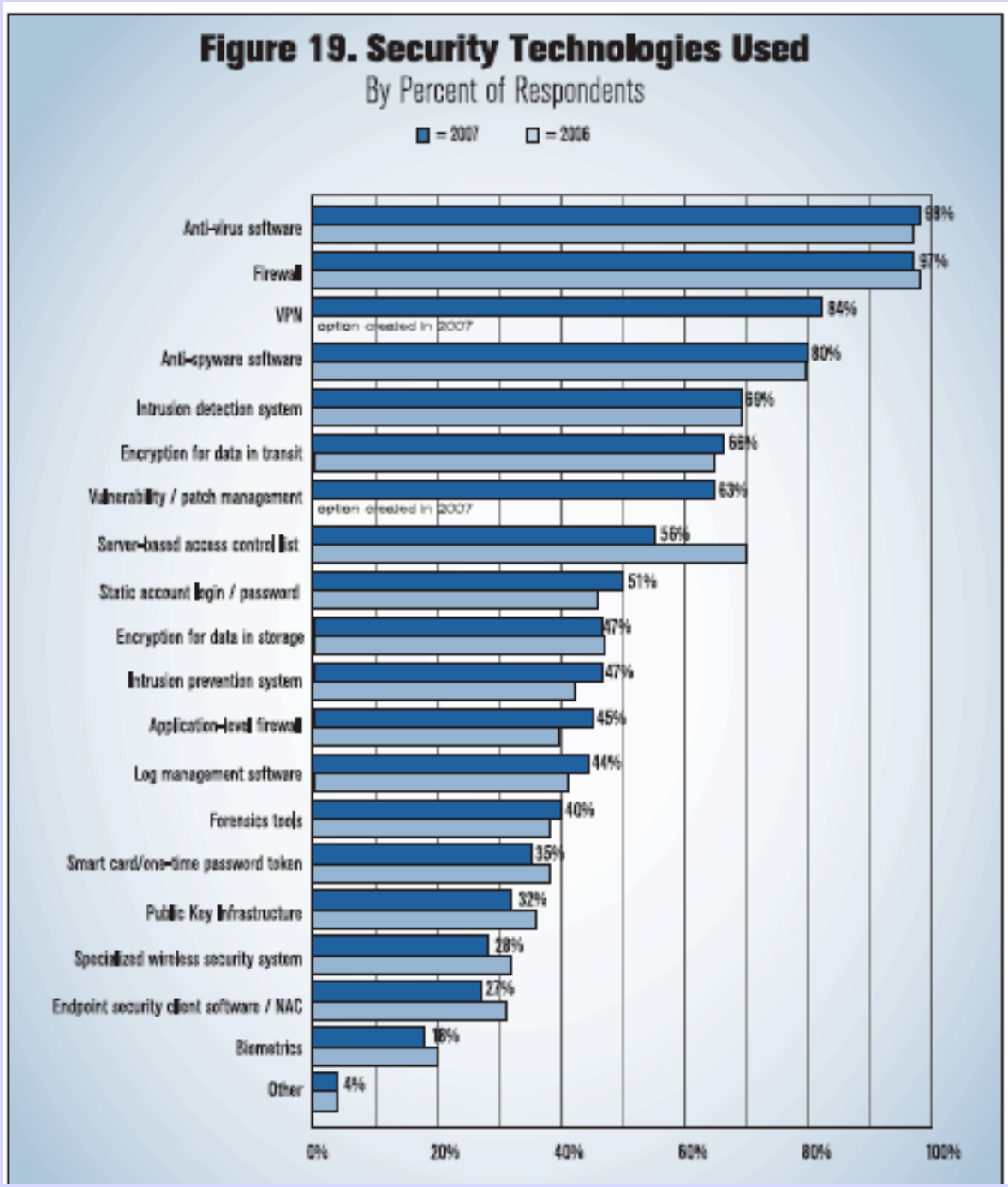
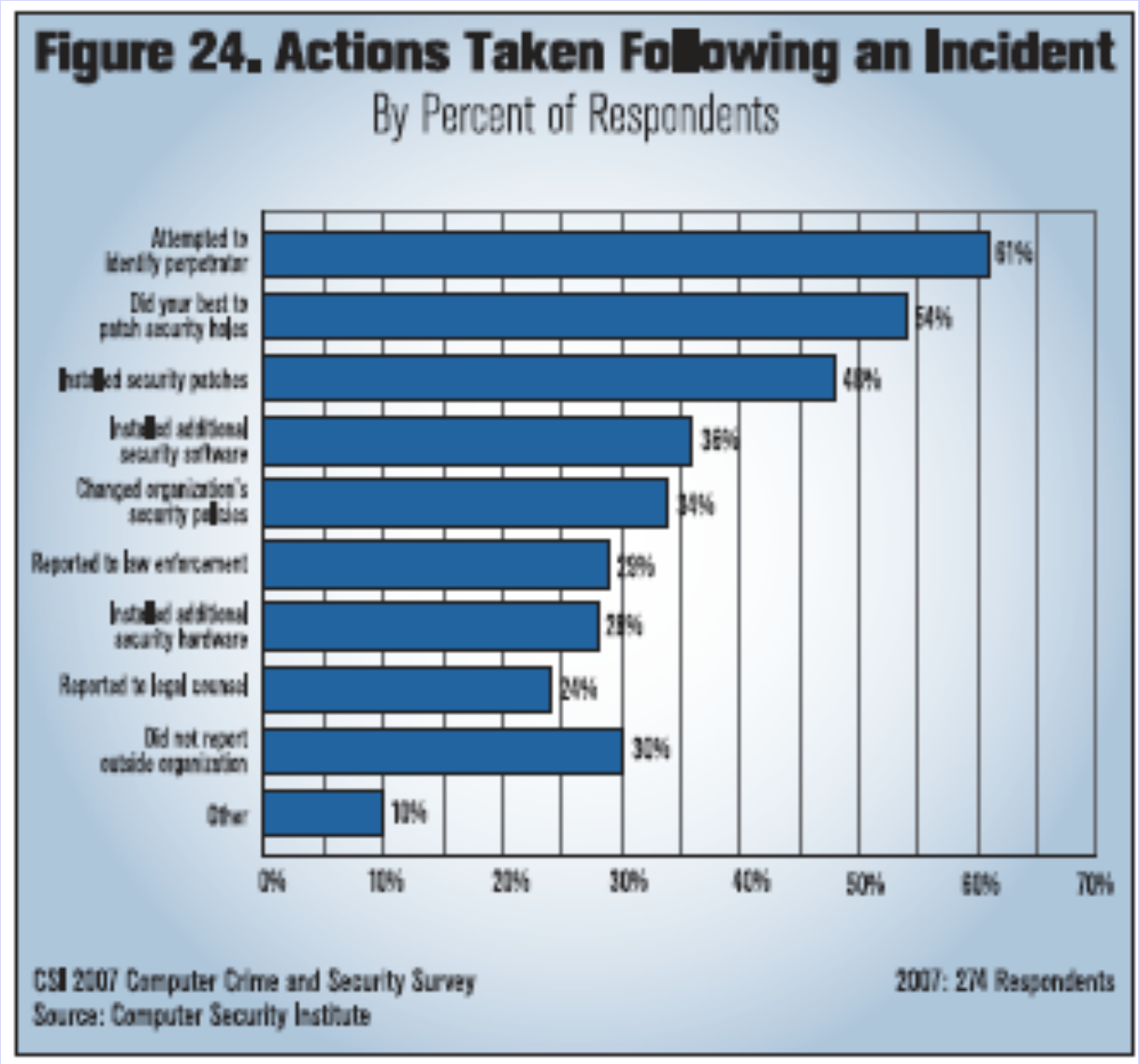


Figure 19. Security Technologies Used
By Percent of Respondents
= 2007
= 2006
Anti-virus software
98%
Firewall
97%
VPN
84%
option created in 2007
Anti-spyware software
80%
Intrusion detection system
69%
Encryption for data in transit
65%
Vulnerability / patch management
63%
option created in 2007
Server-based access control list
56%
Static account login / password
51%
Encryption for data in storage
47%
Intrusion prevention system
47%
Application-level firewall
45%
Log management software
44%
Forensics tools
40%
Smart card/one-time password token
39%
Public Key Infrastructure
32%
Specialized wireless security system
28%
Endpoint security client software / NAC
27%
Biometrics
18%
Other
4%
0%
20%
40%
60%
80%
100%



Decrease in reporting to Law Enforcement

Only 29% reported crimes/attacks

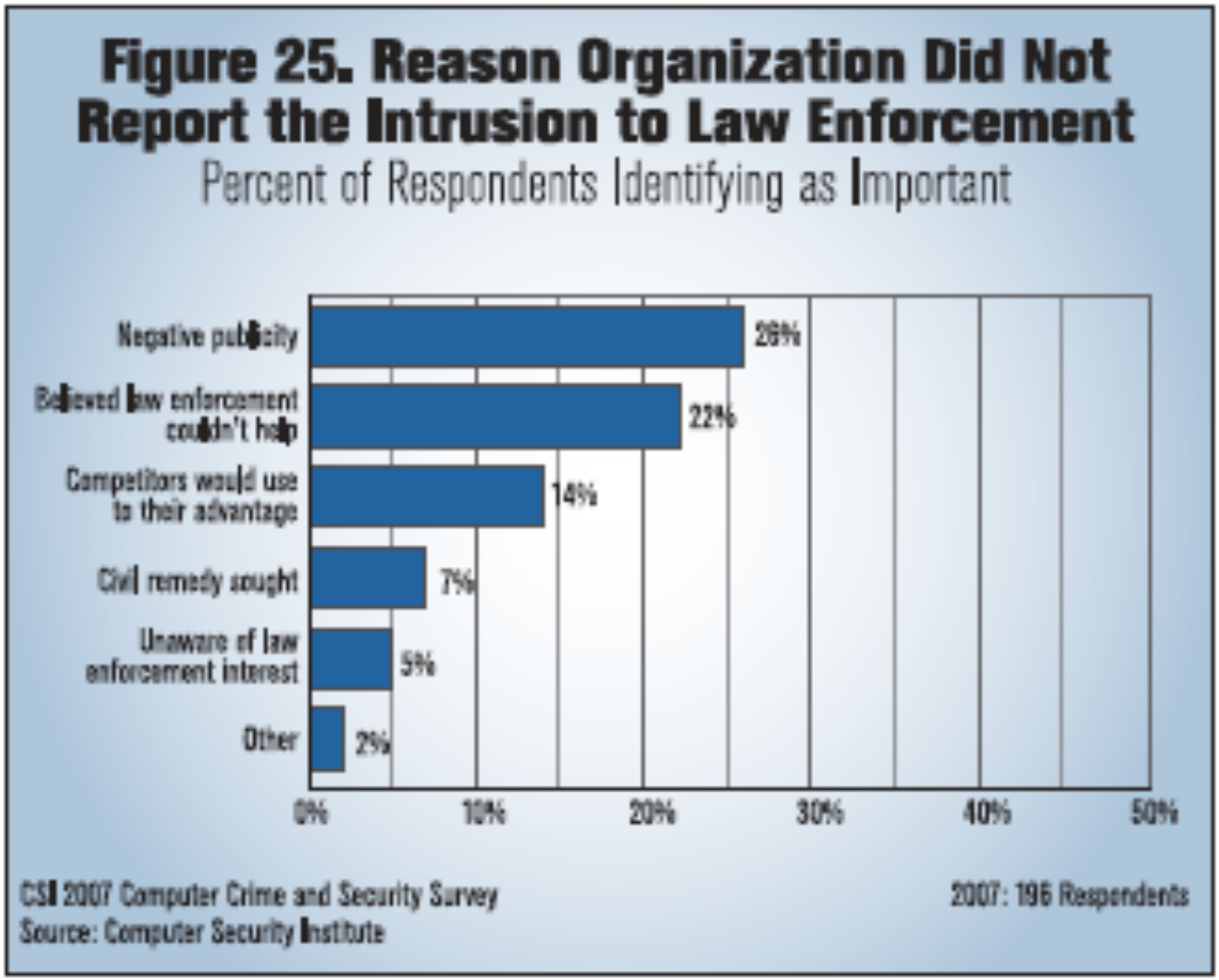


Figure 25. Reason Organization Did Not Report the Intrusion to Law Enforcement
Percent of Respondents Identifying as Important
Negative publicity
Believed law enforcement couldn't help
Competitors would use to their advantage
Civil remedy sought
Unaware of law enforcement interest
Other
28%
22%
14%
7%
5%
2%
0%
10%
20%
30%
40%
50%
CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute
2007: 196 Respondents

Cybercrime

Survey Overview

Slight decrease in overall crime as compared to 2004

Some types of attacks are decreasing, others are increasing

Approximately 80% of all cyberattacks go unreported by companies.

- Fear of negative publicity is biggest reason for non-report

Major financial loses from attacks

- On average $230,000 per survey respondent

Over $14 Billion lost worldwide

Types of Computer Crime

Defining computer crime is a very difficult thing as there are no established crime categories for these types of crimes

Examples of crime categories

1. Old crimes vs. New Crimes
2. Hacking, Cracking, Terrorism:
3. DOJ: Computer crime, Intellectual property crime.
4. Computer centered:
    1. Computer as Target
    2. Computer as Instrument
    3. Computer as incidental
    4. Crimes associated with prevelance of computers

Computer as Target

These type of crimes are based around the computer as the main source of the crime.

While the victim in these attacks can vary from a corporation to an individual, the main target is a particular computer or computers.

Examples:

- **Denial of Service attacks**: Overload webpage servers
    - Financial and political motivations
- **Data alteration**: Attacking information stored on a computer.
    - Destroying, copying confidential files, overwriting files.
- **Computer Vandalism**: Nuisance more than malicious attack of computer.

Computer as Instrument of Crime

These type of crimes are based around the computer as the main instrument of the crime.

While a burglar may use a crowbar as an instrument of crime, a cybercriminal may use a computer to facilitate a particular crime.

Examples:

- Theft: Stealing of data, theft of money from accounts.
  - Salami Slice: Round-down of transactions and divert rounding
- Theft of Services: Getting services for free (internet).
- Fraud: Nigerian Bank scheme.
- Harassment: Stalking and harassing old girlfriends.

Computer as Incidental to a Crime

These type of crimes are ones in which a crime involves the use of a computer simply for ease in maintaining the efficacy of criminal transactions.

Computer is not the primary instrument of the crime, it simply facilitates the crime.

Examples:

- Money Laundering: Used to coordinate and track transactions.
- Counterfeiting: Cannot be done anymore without a computer.
- Criminal Enterprise: Bookies, Mob, criminal gangs.
- Child Pornography: One of the biggest industries on the internet

Crimes Associated with the prevalence of computers

These type of crimes are mainly the computer industry itself, but also include those individuals who have tried to avoid IT all together.

Examples:

- Intellectual Property Offenses: Movies, music, software, etc ..
- Component Theft: Theft of hardware. Laptop theft is huge.
- Identity Theft: Stealing your personal information
- Miscellaneous Corporate Crime: Corporate fraud, rebate fraud, unfair EULA's.

White Collar Crimes

While street crimes garner the majority of the press and public attention in the U.S., White Collar Crime does just as much if not more financial and physical damage.

Technology has been a boon to WCC allowing it to spread to new areas and allowing it to be committed more easily and hidden even better.

In particular, technology has altered the techniques used to commit the most common WCC.

- Embezzlement
- Corporate Espionage
- Money Laundering
- Fraud
- Identity crimes
- Counterfeiting

Embezzlement

What is embezzlement?

Definition: Unlawful misappropriation for personal use of money, property, or some other thing of value that has been entrusted to an offender's care, custody, or control.

Nutshell: Theft in violation of a trust.

Embezzler is usually in some fiduciary relationship with the victim, either as an employee, guardian, or trustee.

Typically, employees steal property or money from a company.

Historical Profile of Embezzler:

- Low level financial institution employee
- Female, bank teller
- Manager of financial affairs of societal elites.

Embezzlement

Often characterized as having more in common with a street robber than with a corporate head.

Embezzlement schemes are often carried out by individual offenders rather than organized entities.

Considered a "computer-assisted" crime because computers are used only in a supporting capacity.

Traditional Methods

- Skimming the till: Overcharging and taking a cut off the top
- Fictitious Employees
- Cooking the books: Inflating and skimming from accounts.
- Fictitious or inflated invoices: $600 toilet seats

Embezzlement

Modern embezzlers are characterized as internal perpetrators who use legitimate access to computers for illegitimate purposes.

Modern Methods

- **Salami Technique**: Slices off small parts of a transaction and diverts it to special account.

  Rounding down: Transactions are rounded down and the remainders are put into another account.

- **Fake Raise**: Authorizing raises to an individual by virtue of "using" a stolen password.

- **Parking**: Putting fund transfers into "created" accounts for short periods of time in order to accrue interest. Funds are then transferred to their real account. Relies on people not being able to calculate interest to the penny.

Embezzlement

Famous Cases:

- **Daniel Gruidl**: Used false passwords in order to log onto the company payroll system and authorize raises and bonuses. Gave himself over $108,000 in raises and wasn't caught for 2 years.
- **Don McCorry**: Altered computer records of employee withdrawals from their retirement accounts by reassigning monies to his retirement account, labeling them "emergency" withdrawals. When arrested police confiscated a Mercedes, a $50,000 art collection, a $100,000 wine collection, and 50 suits valued at $10,000.
- **Frank Gruttadauria**: Defrauded 50 business execs over 15 years. Exaggerated values of client investments by altering financial statements. Clients believed they had assets of $277 million, but accounts actually totaled a little over $1 million.

Corporate Espionage

Definition: Involves any theft of proprietary business information through spying or deception, particularly the theft of "trade secrets".

Trade secrets encompasses any proprietary information that produces value to a commercial enterprise because it provides competitive advantages over business rivals.

Items Stolen:

- Detailed customer lists
- Product specifications
- Research and Development data
- Computer Source codes
- Corporate strategy documents
- Pricing lists
- Technology and computer systems data

Corporate Espionage

How much does this occur?

- Fortune 1,000 companies lost $45 Billion in 1999 alone
- Average company detects 2.45 cases of espionage a year with a cost of $500,000 per incident.
- Fortune 1,000 Technology companies average 67 espionage attacks a year costing an average of 115 million annually.
- National Counter-Intelligence Agency estimates that loses by international spies was $44 Billion in 1997-99.
- Amount has doubled since the early 1990's
- Increase has been most dramatic since the end of the Cold War and the unemployment of high amounts of highly trained spies.

Corporate Espionage

Increasingly this crime has been one of great concern within business circles.

In particular the increased use of e-mail and the huge focus on e-commerce has made corporate espionage much easier to commit.

No longer do corporate thieves have to physically steal information, now they can hack into IT systems and steal e-mail, customer lists, and other important documents.

Availability of former highly trained Military spies makes theft much easier for corporations than previously.

Corporate Espionage Typologies

Insiders: People who have legitimate access to a company's computer networks.

Research suggests 85% of all espionage is insiders.

Largely from job dissatisfaction, money issues, or blackmail.

Outsiders: Domestic spies hired by corporate competitors and foreign nationals hired by rival governments to gain advantage over US companies.

Often involves physical stealing of computers, passwords, or gaining access to server farms.

Contractors: Long-term part-time workers who often have no loyalty to company they are paid to do jobs for.

Often have access to highly important information

Hired or paid by others for information

Corporate Espionage Enforcement

Because of some very public cases costing companies many millions Congress passed the Economic Espionage Act of 1996

Companies that feel they are victims of espionage can request an FBI investigation.

If the investigation reveals any criminal wrongdoings the US attorney's office of the DOJ will prosecute the offending firm.

Crimes Covered by Act

1. **Foreign Espionage**: Those acts originating from foreign governments and businesses.

   Punishment: 500,000 and/or 15 years: Companies 10 million

2. **Domestic Espionage**: Those acts originating from domestic competitors. Makes theft of trade secrets related to or included in a product involved in interstate commerce a federal crimes

   Punishment: $250,000 and/or 10 years.

Corporate Espionage Example

A couple was recently arrested in Britain and extradited to Israel after it was determined they create a Trojan Horse program that was used by companies to spy on their competitors.

Private investigators working for various companies bought the Trojan Horse and set it loose on the competitors computer networks.

The Trojan Horse allowed the P.I's to look around the networks of the competitors for information about the plans and trade secrets of the others.

Companies involved in the espionage include:

- Top 2 cell phone companies in Israel
- Top Satellite cable operator in Israel
- Public relations firm and grocery store firm

Money Laundering

Definition: The act of concealing the source of assets that have been illegally obtained.

Primary objective with money laundering is to hide the source and ownership of such funds through the creation of a seemingly legitimate history or paper trail.

Not a new crime, in that money laundering has been around for many years, but technology has allowed it to grow dramatically

How much is there?

Impossible to know, but estimates are that #300 billion is laundered each year

Drug dealing alone is estimated to launder $5 to $15 billion

Traditional Money Laundering Techniques

1. **Physical:** Illegally obtained cash was physically transported to another jurisdiction with less stringent banking and reporting requirements.

   Cash was lost by Law Enforcement

2. **Conversion**: Cash could be converted into real property such as real estate, commercial interests, or personal luxuries.

   Ostentatious: Purchases often brought attention

   High Amounts: Too much money to spend easily

3. **Smurfing**: Division of large sums of money into smaller sums to conceal their origin. "Smurfs" were then sent out to make small deposits, below $10,000, into different accounts at Banks across a geographic area.

   Avoids reporting problems of large deposits of cash

Technologies impact on Money Laundering

In the 1960's and 70's Governments, Banks, and other financial institutions moved to using electronic means to transfer funds rather than physical means.

These Electronic Funds Transfers (EFT's) served to make it easier for banks to transfer funds, and to also make money laudering much easier.

FedWire: Electronic payment system used by Federal Reserve System.

Over 250,000 transactions a day.

CHIPS: Clearinghouse payment system created by private banking companies.

$866 billion moved each day

**Very difficult to notice money laundering with these kinds of #'s

Money Laundering Example

I am a drug dealer with rooms filed with lots of cash that I need to launder so I can pay my dealers and my mortgage.

I hire a Launderer who hires smurfs to deposit the funds in different accounts at branches of every bank in the central KY area.

They always deposit between $7,500 and $8,500

The launderer then begins to transfer these funds from each branch and depositing the money with Internet banks that accept e-cash

Once the cash becomes converted into e-cash the money has become virtually untraceable-anonymous

I now have access to legitimate e-cash.

Money Laundering Enforcement

Two main laws that deal with money laundering

1. **Bank Secrecy Act of 1970**: Requires banks to file records concerning suspicious financial transactions over $10,000.

2. **Money Laundering Control Act**: Requires banks and other financial institutions to report ANY suspicious banking transactions.

    Includes possible smurfing schemes regardless of the amount

Main Law Enforcement assistance comes from Treasury Department's Financial Crime Enforcement Network (FinCEN)

Main objective is to provide law enforcement with tools they necessary to identify and prosecute money laundering cases.

FinCEN

Counterfeiting

- The counterfeiting of money is one of the oldest crimes in history at some periods in early history, it was considered treasonous and was punishable by death.
- During the Civil War, one-third to one-half of the currency in circulation was counterfeit. At that time, approximately 1,600 state banks designed and printed their own bills. Each bill carried a different design, making it difficult to detect counterfeit bills from the 7,000 varieties of real bills.
- A national currency was adopted in 1862 to resolve the counterfeiting problem. However, the national currency was soon counterfeited and circulated so extensively that it became necessary to take enforcement measures.
- Therefore, on July 5, 1865, the United States Secret Service was established to suppress the wide-spread counterfeiting of this nation's currency.
- Today, counterfeiting once again is on the rise. One reason for this is the ease and speed with which large quantities of counterfeit currency can be produced using modern photographic and printing equipment.

Counterfeiting

How Much of a problem is counterfeiting?

- Of the $380 billion in U.S. currency circulated in fiscal year 1994, $208.7 million was counterfeit.
  - This amount represented less than one one-thousandth of U.S. currency in circulation at that time.
- From 1995 to 2000 the amount of domestically seized counterfeit currency rose from $174,924 to $18,426,000.
  - 94% of the domestic based counterfeiting was digitally created
- Half of the counterfeit currency being distributed in the U.S. is "muled" into the U.S. from foreign countries, with Colombia being the number one producer.
- In general the U.S.S.S is seeing an increase due to the increased technology making it easier for less skilled criminals to produce high quality counterfeit bills.

Counterfeiting

Methods of Counterfeiting

1. **Engraving**: Traditional method of counterfeiting where an engraver created a new set of plates for printing money.
   Problematic in that it required a great deal of skill.
2. **Offset Lithography**: A presensitized aluminum plate is exposed under a photographic negative of the note Chemicals on the pretreated plate react and an image of the note appears on the plate To print, the plate is moistened with water, which repels the ink from the nonprinting surface The image is then inked and transferred to a rubber blanket roller which puts it on the paper.
   Expensive materials but fairly easy to do for amateurs.
3. **Photocopy**: With the advent of high quality scanners, printers and photographic paper, this method is increasingly popular.
   These bills are often passed in change making machines that use a scanning process to validate bills.

Counterfeiting

4. **Raising**: Uses a legitimate bill but they "raise" the value of the bill. Commonly done with $1 to a $10.
   Abrasives are used to remove the denomination and other note markings and then pen and ink are used to fill in the holes.
5. **Paster**: A counterfeiter tears the corners of of good bills (not all from the same bill) until they have 4 corners which they then pastes on a good note of a smaller denomination.
   Requires access to legitimate bills.
6. **Bleaching**: Small denomination notes are bleached until all or part of the ink is removed from the paper and then new values are printed on the bleached paper.
   Popular technique because of the real feel of the money, but it still requires a good plate or printer.

Detecting Counterfeit Money

Portrait: The genuine portrait appears lifelike and stands out distinctly from the background. The counterfeit portrait is usually lifeless and flat. Details merge into the background which is often too dark or mottled.

REAL

Detecting Counterfeit Money

Federal Reserve and Treasury Seals: On a genuine bill, the saw-tooth points of the Federal Reserve and Treasury seals are clear, distinct, and sharp. The counterfeit seals may have uneven, blunt, or broken saw-tooth points.

REAL

Detecting Counterfeit Money

Border: The fine lines in the border of a genuine bill are clear and unbroken. On the counterfeit, the lines in the outer margin and scrollwork may be blurred and indistinct.

REAL

Detecting Counterfeit Money

Serial Numbers: Genuine serial numbers have a distinctive style and are evenly spaced. The serial numbers are printed in the same ink color as the Treasury Seal. On a counterfeit, the serial numbers may differ in color or shade of ink from the Treasury seal. The numbers may not be uniformly spaced or aligned.

REAL

New Money

Because of new technologies making it easier to counterfeit the U.S. Gov has released new money with new technologies.

- Color: Orange, yellow, red
- Color shifting ink
- Water mark
- Security thread
- Microprinting

New Security Features

Security Thread

Hold the note up to the light and look for the security thread, or plastic strip, that is embedded in the paper and runs vertically to the right of the portrait. If you look closely, the words "USA TEN" and a small flag are visible along the thread from both sides of the note. This thread glows orange when held under ultraviolet light. In the redesigned $10 note, the thread has shifted slightly to the right of its location on older series $10 notes.

Color-Shifting Ink

Look at the number "10" in the lower right corner on the face of the note. When you tilt the note up and down, the color-shifting ink changes color from copper to green.

Watermark

Hold the note up to the light and look for the watermark, or faint image, similar to the large portrait of Treasury Secretary Alexander Hamilton. The watermark is part of the paper itself and can be seen from both sides of the note. A blank oval has been incorporated into the new $10 design to highlight the watermark's location.

Law Enforcement and Counterfeiting

The Secret Service has exclusive jurisdiction for investigating counterfeiting in the U.S.

In addition to investigation of paper money counterfeiting, the U.S.S.S also investigates:

- Counterfeit coins
- U.S. Treasury checks
- Department of Agriculture food coupons
- Postage stamps

The U.S.S.S works closely with local, state, and international law enforcement agencies.

They, more than some other agencies, have a need for people with technological expertise due to the constant change in reprographic and lithographic technology (printers, scanner, copiers).

Identity Theft

What is it: Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes.

Most often identity theft involves the use of a stolen S.S. # to create false bank accounts, open credit cards, purchase goods and generally ruin an individuals credit rating.

Federal government often lumps this crime in with other types of Fraud

How Big of a problem is ID Theft?

Estimates are difficult to determine because of the way it is categorized as fraud and grouped with other figures.

Thus, it is important to take the figures that you read about ID Theft as estimates of the problem and remember that they are often used for political and/or financial reasons.

Identity Theft

Estimates of the problem

- Personal loses due to ID Theft were around $745 million in 1997, a 68% increase in loses tied to ID Theft in a 2 year time period.
- Approximately 350,000-500,000 people a year experience some monetary loss connected to ID Theft.
- FTC reported that in 2004 53% of all fraud complaints were internet related and resulted in loses of $265 million.
- In 1999 the Social Security Administration received over 62,000 allegations involving the misuse of S.S. # alone.
- From May 2004-May 2005, 2.4 million people were victimized by Phishing, with an estimated loss of $929 million.
- The Secret Service's Financial Crimes Division reported that loses related to ID Theft in 2000 were over $248 million.
    - Other estimates put loses around $1.5 Billion.

- Overall, no matter the source all estimates indicate that there has been an increase in ID Theft over the past 5 years

Identity Theft

Why has there been an increase in ID Theft?

1. **Social Security #'s**: The S.S. # has become the most used I.D. # in the U.S. putting it at increased susceptibility to being stolen and used for illegal purposes.

   Used for ID in an increasing number of situations where it was never intended to be used.

2. **E-Commerce**: We are increasingly giving out bank, credit card , and other financial numbers over the internet.

With each increased use we are increasing the likelihood that numbers will be obtained fraudulently

**Many times the two are combined in that we give out our S.S. # with our bank or credit card number.

Methods of Identity Theft

1. **Dumpster Diving:** Rummaging through an individuals garbage looking for personal information about them.

Once garbage is at the street and off your property it is considered fair game for anyone to look through.

2. **Mail Theft**: Stealing a persons mail in order to get personal information.

- Stealing mail itself is a federal crime.

3. **Shoulder Surfing**: Looking over a person's shoulder in order to steal information or important numbers.

- Airports, DMV, anyplace you need to fill out forms with important information, or where people have to say their S.S. #

4. **Phishing**: Sending of e-mails that seem to be real in order to dupe people in to providing important information.

- Banks, e-bay, credit cards, amazon, etc..
- Work because many of the fake sites are very real looking.

Methods of Identity Theft

5. **Hacking:** Breaking into a protected corporate server and stealing information.
- Banks, data aggregators, Universities, and other organizations that store large amounts of personal information.
6. **Phone Solicitation**: Calling and pretending to be from a bank or other important service company.
- Variation on phishing but still very popular method especially amongst the elderly.
- Phone lists often come from obituaries and prey on families in mourning.
7. **Buying S.S. #:** Some websites contain information about how and where to buy S.S. #.
8. **Pick Pocket**: Steal and walet and quickly go and purchase gift cards with stolen credit cards.
- Sell the gift cards for cash or use them to purchase gifts.
- Laundering of credit cards before they can be cancelled.

Methods of Identity Theft

9. **Trojan Horses**: Malicious files that infiltrate your PC by hiding in seemingly innocuous documents.
- Some trojans, called keystroke loggers, record your keystrokes and send them to an offenders computer.
10. **Zombie Computers**: Remote-access Trojans (RAT's) install hidden code that allows your PC to be controlled remotely.
- Thieves then use robot networks of thousands of zombie computers to carry out attacks, send spam, etc..
11. **Man in the middle Attacks**: Hackers pose as online banks or merchants, letting victims sign in over a Secure Sockets Layer connections (SSL).
- Offender then logs into the real server using the client's information and steals credit cars info. And bank information.
12. **URL Obfuscation**: Taking advantage of human error, some phishing e-mails guide users to fake sites with similar names.
- monneybank.com vs. moneybank.com

Methods of Identity Theft

13. **DNS Cache Poisoning**: The Domain Name System (DNS) is like an internet phone book that translates host names such as "eku.edu", into IP addresses such as 208.184.224.88 (these numbers actually make the connection).
- A DNS-Cache Poisoning attack changes entries in the victim's copy of the phone book, so when they type a legitimate site name they are sent to a fake address.

14. **Pharming**: Using tricks such as DNS cache poisoning, pharming redirects visitors from a real site to a fake site.
- Once directed to this fake site crucial information is stolen.

15. **Evil Twins**: An "evil twin" is a fake wireless internet hot spot that looks like a legitimate service.

* When a victim connects, the hacker can launch man-in-the-middle attacks on transactions on the internet, or just ask for credit card information in the standard pay-for-access deal.

Perpetrating Identity Theft

Once you have a S.S. #, an address and name you can pretty much do anything.

Most often criminals will do one of the following:

- Credit card account
- Bank account
- Purchase cars and houses

Once you have an account set up in someone elses name you can pretty much wreck havoc on an individuals credit score.

** Importantly, once a credit score has been wrecked it is difficult and expensive to fix it.

Enforcing Identity Theft Crimes

In 1998 Congress passed the Identity Theft and Assumption Deterrence Act

This law makes it a federal crime when someone:

"Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or aid or abet, any unlawful activity that constitutes a violation or federal law, or that constitutes a felony under any applicable state or local law."

Violations of the law may be punishable by up to 15 years in prison

**Reality of this law is that is largely symbolic as ID Theft is very difficult to investigate properly and prosecute.

These cases are very labor intensive and require a great deal of collaboration across different levels of law enforcement.

Many think that private means are the best way to prevent problems

Protecting Yourself from ID Theft

While this is not a guarantee that you will be safe from ID Theft, these tips will help reduce your likelihood of being a victim.

1. **Clean PC**: Keep your PC clean by keeping your antivirus and spyware software up to date and scan your computer regularly.
2. **Firewall**: Enable windows built in firewall or purchase a router with a built-in firewall.

- Make sure when you set up the firewall that you change the default password and ID.

3. **Be Smart**: Be wary of e-mail asking you to provide personal or financial information.

- As a rule NEVER trust an e-mail about a bank or other online account needing to be updated. You can always do it in person or drop the service.

4. **Be Smart II**: If you don't know who sent it or what it is don't click on it.

- Look at the extension to try and figure out if it is a program or document.

Protecting Yourself from ID Theft

5. **Look for "Ticks":** Thoroughly check your bank account and credit card statements carefully.
- Scammers often make charges of $20 or less to avoid detection.
- Get a free copy of your credit report to check for suspicious activity
-

6. **Paper trail**: Get a cross shredder and destroy unwanted credit card and loan applications that come in the mail.
- Dumpster diving is easy on college campuses and large apartment complexes.

7. **Act Quickly**: If your ID is stolen file a fraud alert on your credit report by calling Equifax, TransUnion, or Experian.
- After filing the alert call your credit card company quickly.

Identity Theft Industry

As with many crimes that are seen as being out of control, regardless of whether they are, identity theft has developed into a major economic industry.

Countless companies, security professionals, and consultants make billions of dollars offering security, protection, safety, and piece of mind.

Examples of the IDT Industry

- **Credit report security and warning systems**: For a monthly or yearly fee these companies will monitor the three major credit rating systems for changes to your credit rating and provide you with alerts if anything changes abruptly.
- **Security Consultants**: Consult with industry, teach seminars, write books on how to protect yourself from ID Theft.
- **Stand alone Products**: Products designed to prevent common problems associated with ID Theft.

Credit Report and Security Warning Systems

Most well known of all of the different companies is Equifax

Main Products

Credit Report Watch: Regularly checks your credit report for changes you did not make

Automatically alerts you within 24 hours of key changes in your Equifax Credit Report, like when someone tries to get credit in your name, so you can act before serious damage is done.

Equifax Credit Watch: Can alert you to sudden changes in your credit card balances.

Credit card fraud is most common fraud

$20,000 of Identity Fraud Expense Coverage with no deductible, certain limitations and exclusions apply, at no additional charge to you.

Security Consultants/Experts

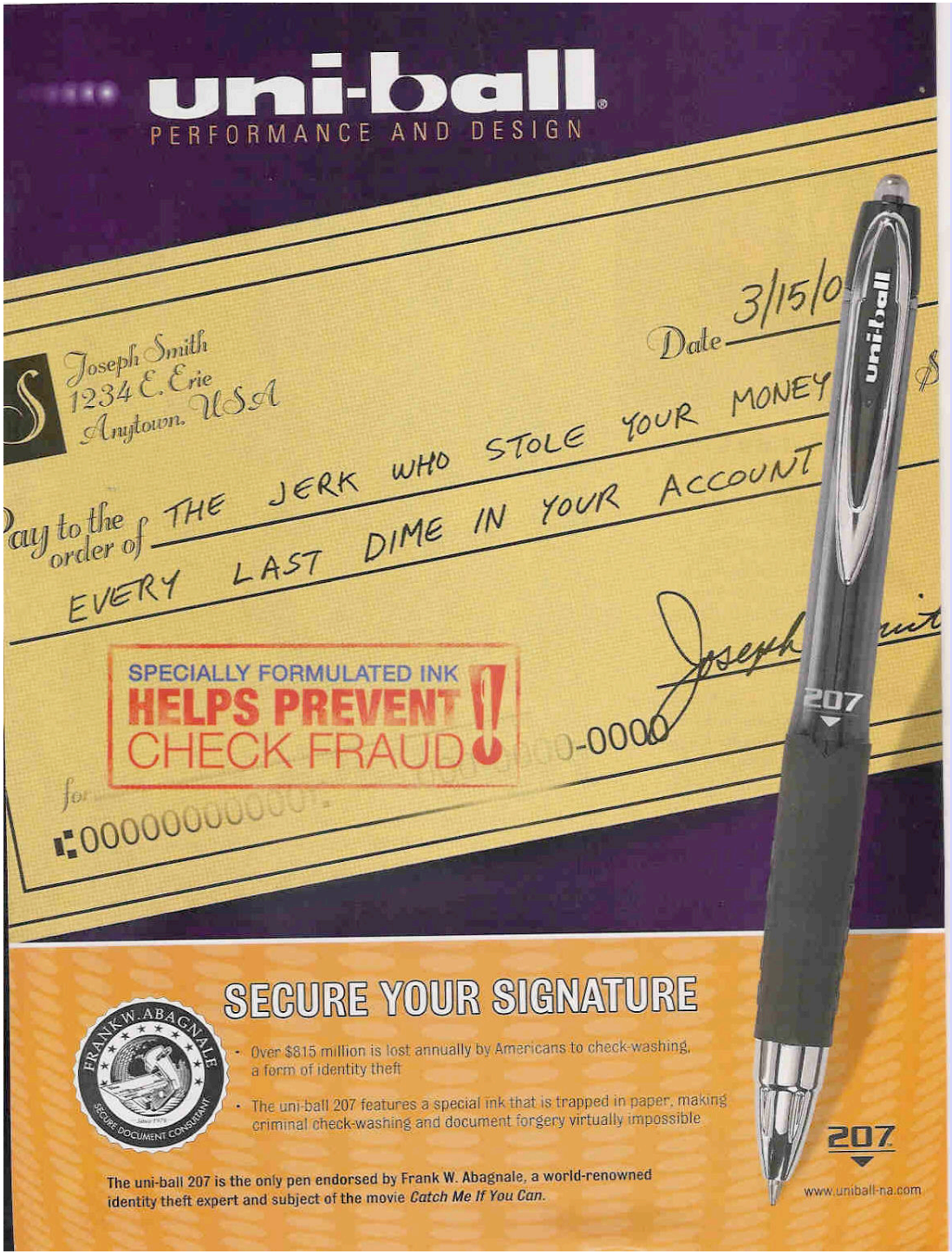
The best know security consultant is Frank Abagnale of "Catch me if you can" fame.

Services

- In-house consulting
- Negotiable document reviews
- Document design
- Specialized training
- Informative Seminars

Books

- Catch Me if You Can
- Art of the Steal
- Real U Guide to Identity Theft



Stand Alone Products

Ad from Money Magazine

- Fear inducing numbers of victims
- Solution with their product
- Endorsement from famous security professional

Stand Alone Products

The uni-ball 207 uses an ink that contains color pigments, which are absorbed into a check's paper fibers. When an individual tries to "wash" the information written on the check, the ink is in effect trapped. The uni-ball 207 retails for just over $2.00. Refills are available. Uni-ball 207 is sold worldwide in major stationery and office supply stores and other outlets.

Not only is this a great solution, it is an inexpensive way to protect your self from being one of the millions of victims.

Identity Theft Examples

Credit History: Federal agents arrested a former employee at a Long Island software company who allegedly originated a crime ring that eventually cost consumers $2.7 million.

Suspects sold credit reports of over 30,000 people, including names, S.S. #'s, and other credit information to identity thieves.

Thieves used this information to fraudulently obtain a wide variety of consumer goods.

Each victim's credit history was sold for only $30.

Military Identity: An individual was sentenced to 41 months for fraudulently obtaining the names and S.S.#'s of high ranking military officers from internal government web sites.

He then used this information to apply on line for credit cards and other lines of credit.

Identity Theft Examples

Choice Point: In February 2004, this data aggregator was "conned" into giving up sensitive data on on 145,000 people within its database.

CardSystems Solutions: In 2005 this transaction processing company ($15 billion in Debit and Credit Card transactions a year) had a hacker break-in that potentially exposed 40 million debit and credit card accounts.

- An investigation showed that the company failed to follow the credit card industry's own security standards and was thus an easy target.
- It is unknown what the potential damage of this hack is.

Internet Fraud

Old school crime that has found new life on the internet thanks to the ability to easily solicit thousands of people.

Relies to some degree on people being naïve of a plot.

Most of the frauds committed on-line are simply new takes on old schemes

- Chain letter hoaxes and urban legends
- Confidence schemes
- Bait and switch con games
- Auction fraud
- Investment fraud

Amount of Fraud

- Complaints to National WCC Center increased 400% from 2000-02
- Auction fraud accounts for 64% of all fraud complaints with over 30,000 complaints a year.
    - Approximately $4 million lost a year ($780 a person)

Internet Fraud

1. **On-line Auction Fraud**: Defrauding an individual involved in an on-line auction.

- Most common method is non-delivery of goods.
- Misrepresentation of goods
- Shill Bidding: Intentional fake bidding to inflate the price.
- Fee Stacking: Seller adds hidden charges to the cost of the item prior to delivery, most often through shipping costs.

2. **Nigerian Bank Scheme**: Also called the "419" scam because of the Nigerian Criminal codes violated in the scam.

- Since its inception in 1989 it is estimated that the loses are $1 billion globally.
- The Internet Fraud Compliant Center received 16,000 complaints alone in 2002.

Nigerian Bank Scam

From the Desk of:
Mr. John O. Aboh
Banking Operations,
First Bank Of Nigeria Plc.,
Lagos-Nigeria.

Dear Sir,
STRICTLY A PRIVATE BUSINESS PROPOSAL

I am Mr. John O. Aboh, The Executive Director, Banking Operations of the First Bank Of Nigeria Plc.

I am writing this letter to ask for your support and cooperation to carry out this business opportunity in my department.

We discovered an abandoned sum of $15,000,000.00 (Fifteen million United States Dollars only)in an account that belongs to one of our foreign customers who died along with his entire family of a wife and two children in November 1997 in a Plane crash.

Nigerian Bank Scam

Since we heard of his death, we have been expecting his next-of-kin to come over and put claims for his money as the heir, because we cannot release the fund from his account unless someone applies for claim
as the next-of-kin to the deceased as indicated in our banking guidelines.

Unfortunately, neither their family member nor distant relative has ever appeared to claim the said fund. Upon this discovery, I and other officials in my department have agreed to make business with you and release the total amount into your account as the heir of the fund since no one came for it or discovered he maintained account with our bank, otherwise the fund will be returned to the banks treasury as unclaimed fund.

We have agreed that our ratio of sharing will be as
stated thus;

20 % for you as foreign partner,
75 % for us the officials in my department and
5 % for the settlement of all local and foreign
expenses incurred by us and you during the course of
this business.

Nigerian Bank Scam

Upon the successful completion of this transfer, I and one of my colleagues will come to your country and mind our share. It is
from our 75 % we intend to import Agricultural Machineries into my country as a way of recycling the fund. To commence this transaction, we require you to immediately indicate your interest by a return e-mail and enclose your private contact telephone number, fax number full name
and address and your designated bank coordinates to enable us file letter of claim to the appropriate departments for necessary approvals before the transfer can be made.

Note also, this transaction must be kept STRICTLY
CONFIDENTIAL because of its nature.

I look forward to receiving your prompt response.

Mr. John O. Aboh
Banking Operations,
First Bank Of Nigeria Plc.,
Lagos-Nigeria.

Internet Fraud

3. **Chain Letter Hoaxes/Urban Legends**: Online version of an old scam designed to get people to forward an e-mail as many times as possible.

Often these scams ask people to forward the e-mail to as many people as possible with the promise of $ for each time its forwarded.

Not much cost associated with these, rather it just makes you feel stupid for thinking you'll actually get money for this.

- Microsoft is testing new e-mail, everyone gets a Disney World trip
- Outback Steak House is giving away free dinner with every 20 forwards.

Urban Legends can have the impact that they cause a downturn in business due to supposed bad policies that need to boycotted.

- McDonalds, Burger King, etc..

Urban Legends

Subject: SAFETY ALERT - Mobile Phones and Refueling Don't mix

What's the problem: The Shell Oil Company recently issued a warning about three incidents where Mobile Phones have ignited fumes while being answered or ringing during fueling operations.What specifically happened

- Case 1
  The phone was placed on the car's trunk lid during fueling, it rang and the ensuing fire destroyed the car and the gasoline pump.
- Case 2
  An individual suffered severe burns to their face when fumes ignited as they answered a call while refueling their car.
- Case 3
  An individual suffered burns to the thigh and groin as fumes ignited when the phone, which was in their pocket, rang while they were fueling their car.

What should you learn from this?

- It is a misconception that Mobile Phones are intrinsically safe and can't ignite fuel/fumes
- Mobile phones that light up when switched on, or when they ring, have enough energy released to provide a spark for ignition
- Mobile phones should not be used in filling stations, or when fueling lawn mowers, boats etc.
- Mobile phones should not be used around other materials that generate flammable or explosive fumes or dust (i.e. solvents, chemicals, gases, grain dust etc.)
- Mobile phones should be turned off before entering an area where other materials that generate flammable or explosive fumes or dust is located.

Please share this with employees who do not have access to email, family members and friends to help keep everyone safe.

Have a wonderful day!

Urban Legends

This is nuts!!!

Police officers working with the DARE program has issued this warning: If you are driving after dark and see an on-coming car with no headlights on, DO NOT FLASH YOUR LIGHTS AT THEM!

This is a common Bloods gang member "initiation game" that goes like this:

The new gang member under initiation drives along with no headlights, and the first car to flash their headlights at him is now his "target". He is now required to turn around and chase that car, then shoot and kill every individual in the vehicle in order to complete his initiation requirements.

Police Depts across the nation are being warned that September 23rd and 24th is the "blood" initiation weekend. Their intent is to have all the new bloods nationwide drive around on Friday and Saturday nights with their headlights off. In order to be accepted into the gang, they have to shoot and kill all individuals in the first auto that does a courtesy flash to warn them that their lights are off. Make sure you share this information with all the drivers in your family!

Please Foward this message to all your friends and family members to inform them about this initiation ritual. You can save someone's life if you heed to this warning.

The End