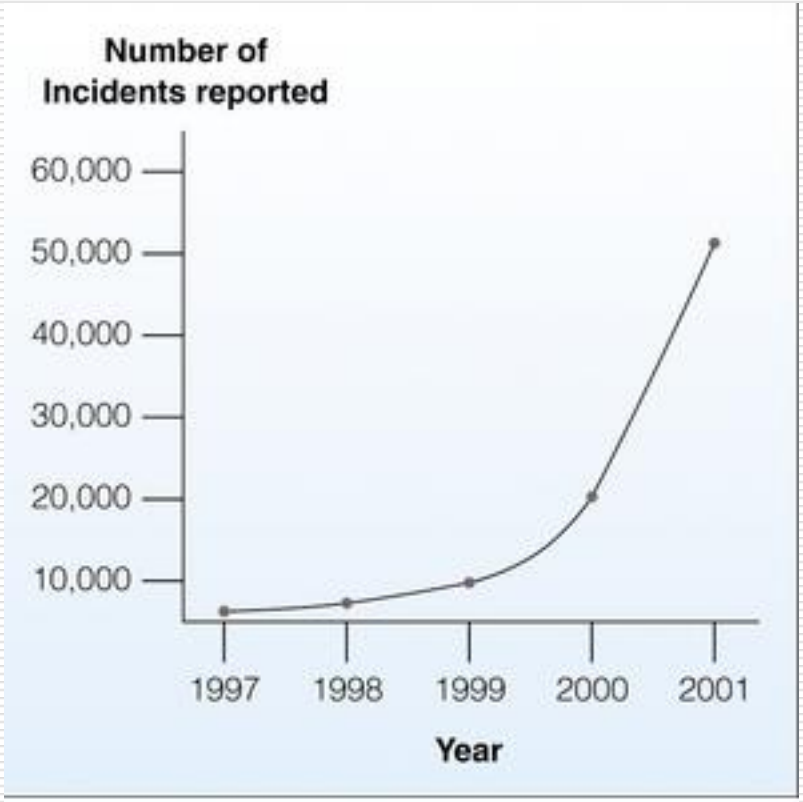
Computer Crime

Number of Incidents Reported to Computer Emergency Response Team (CERT)



Computer Crime and Security Survey

Incident	2002 Results
Respondents that detected computer security breaches within the last 12 months	90%
Respondents that acknowledged financial losses due to security breaches	80%
Average dollar loss of the 44% who were willing or able to quantify their financial losses	$2.0 million
Respondents that cited their Internet connection as a frequent point of attack	74%
Respondents that cited their internal systems as a frequent point of attack	33%
Respondents that reported intrusions to law enforcement	34%
Respondents that detected computer viruses	85%

The Computer as a Tool to Commit Crime

- Social engineering
  - E.g. pre-texting, phishing (email)
- Dumpster diving
  - To get sensitive personal information such as address, password, credit card numbers, etc.
- Identity theft
- Cyberterrorism

Computers as Objects of Crime

- Illegal access and use
  - Hackers
  - Crackers
- Information and equipment theft
- Software and Internet piracy
- Computer-related scams
- International computer crime

How to Respond to a Security Incident

- Follow your site's policies and procedures for a computer security incident. (They are documented, aren't they?)
- Contact the incident response group responsible for your site as soon as possible.
- Inform others, following the appropriate chain of command.
- Further communications about the incident should be guarded to ensure intruders do not intercept information.
- Document all follow-up actions (phone calls made, files modified, system jobs that were stopped, etc.).
- Make backups of damaged or altered files.
- Designate one person to secure potential evidence.
- Make copies of possible intruder files (malicious code, log files, etc.) and store them off-line.
- Evidence, such as tape backups and printouts, should be secured in a locked cabinet, with access limited to one person.
- Get the National Computer Emergency Response Team involved if necessary.
- If you are unsure of what actions to take, seek additional help and guidance before removing files or halting system processes.

Data Alteration and Destruction

- Virus
- Worm
- Logic bomb
- Trojan horse

The Six Computer Incidents with the Greatest Worldwide Economic Impact

Year	Code name	Worldwide Economic Impact
2001	Nimda	$.635 billion
2001	Code Red	$2.62 billion
2001	SirCam	$1.15 billion
2000	ILOVEYOU	$8.75 billion
1999	Melissa	$1.10 billion
1999	Explorer	$1.02 billion

Top Viruses – July 2002

Rank	Virus	Partial Description	Percentage of Virus Occurrences Confirmed
1	Worm/Klez.E	If the system date is an odd-numbered month (January, March, etc.) and the day is the 13th, the virus starts scanning local disks (or drives on the network) and fills the files it finds with random data, permanently destroying them.	57.3%
2	W32Elkern.C	The virus monitors all running applications, and if there are any applications belonging to an antivirus program, it closes them.	16.8%
3	Worm/W32.Sircam	The virus displays a screensaver with a multicolor message that shakes the screen after it is complete. The display messages are: True Love never Ends U r My Best Friend U r so cute today #!#!	4.4%
4	W32/Yaha.E	The virus arrives as an e-mail with an attachment that begins with one of the following names: loveletter, resume, love, weeklyreport, goldfish, report mountan, biodata, dailyreport, love-greentings, or shakingfriendship	4.2%
5	W32/Nimda	The virus arrives through e-mail as an attached file with the name README.EXE. The body of the message appears empty but actually contains code to execute the virus when the user views the message.	2.6%
6	Worm/Frethem.L	The virus arrives as an e-mail attachment that, when the attachment is opened, collects e-mail addresses from the Windows Address Book and files with .DBX, .MBX, .EML, .WAB, and .MDB extensions. It then sends infected messages.	2.2%
7	W32.Magistar.B	The virus checks for existence of the ZoneAlarm firewall software and, if it exists, terminates it.	2.0%
8	Others		10.5%

Preventing Computer-Related Crime

- Crime prevention by state and federal agencies
- Crime prevention by corporations
  - Public Key Infrastructure (PKI)
  - Biometrics
- Anti-virus programs

Preventing Computer-Related Crime

- Intrusion Detection Software
- Managed Security Service Providers (MSSPs)
- Internet Laws for Libel and Protection of Decency

Preventing Crime on the Internet

- Develop effective Internet and security policies
- Use a stand-alone firewall with network monitoring capabilities
- Monitor managers and employees
- Use Internet security specialists to perform audits

Common Methods Used to Commit Computer Crimes

Methods	Examples
Add, delete, or change inputs to the computer system.	Delete records of absences from class in a student's school records.
Modify or develop computer programs that commit the crime.	Change a bank's program for calculating interest to make it deposit rounded amounts in the criminal's account.
Alter or modify the data files used by the computer system.	Change a student's grade from C to A.
Operate the computer system in such a way as to commit computer crime.	Access a restricted government computer system.
Divert or misuse valid output from the computer system.	Steal discarded printouts of customer records from a company trash bin.
Steal computer resources, including hardware, software, and time on computer equipment.	Make illegal copies of a software program without paying for its use.
Offer worthless products for sale over the Internet.	Send e-mail requesting money for worthless hair growth product.
Blackmail executives to prevent release of harmful information.	Eavesdrop on organization's wireless network to capture competitive data or scandalous information.
Blackmail company to prevent loss of computer-based information.	Plant logic bomb and send letter threatening to set it off unless paid considerable sum.

How to Protect Your Corporate Data from Hackers

- Install strong user authentication and encryption capabilities on your firewall.
- Install the latest security patches, which are often available at the vendor's Internet site.
- Disable guest accounts and null user accounts that let intruders access the network without a password.
- Do not provide overfriendly log-in procedures for remote users (e.g., an organization that used the word *welcome* on their initial log-on screen found they had difficulty prosecuting a hacker).
- Give an application (e-mail, file transfer protocol, and domain name server) its own dedicated server.
- Restrict physical access to the server and configure it so that breaking into one server won't compromise the whole network.
- Turn audit trails on.
- Consider installing caller ID.
- Install a corporate firewall between your corporate network and the Internet.
- Install antivirus software on all computers and regularly download vendor updates.
- Conduct regular IS security audits.
- Verify and exercise frequent data backups for critical data.

Internet Security Threads

- Viruses and hostile Web applications (e.g. Java Applets or ActiveX controls)
- Trojan horses
- Adware and spyware
- Spam emails
- Identity theft and spoofing
- Social engineering

Internet Security Measures

- Firewall
- Antivirus software
- Email encryption
- Encryption and authentication
- Frequent updates of software
- Always beware of incoming threads

Antivirus Software

- Symantec: Norton Antivirus, Norton Internet Security, etc.
- McAfee: McAfee Virus Scan, McAfee Internet Security, etc
- Kaspersky
- Bit defender
- BKAV
- …