

Learning to Transfer Your Unwanted Internet & Technology (Network) Risks and Exposures





Technology Insurance Coverage

- There is a great deal of misunderstanding about the extent of coverage provided by traditional insurance policies
- Coverage for technology is very specific
- Technology coverage is specifically designed to provide coverage not presently found in other policy forms



Does my traditional business insurance cover technology risks and exposures?

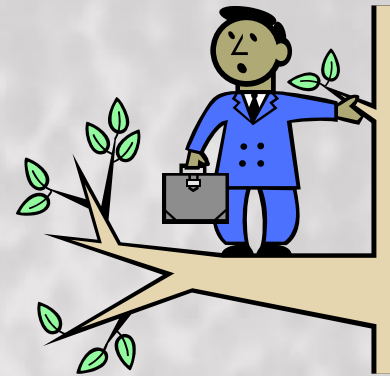
- Traditional business insurance policies are silent on technology coverage or exclude these exposures
- You must have a physical loss to trigger a claim on traditional business insurance
- Traditional business insurance was never intended to cover technology risks, so it doesn't!



Why do you need technology insurance?

- **To transfer the unwanted risks and exposures created by technology that are excluded by traditional business insurance, such as:**

- Loss of revenue
- Breach of security (database)
- Virus
- Theft of credit information
- Loss of intellectual property
- Identity theft



Who really needs technology insurance?

- **Businesses that are in the technology business**
 - Software developers, web designers, systems integrators, ASP, ISP, computer programmers, etc.
- **Businesses that use technology**
 - Brick & mortar businesses that use technology, i.e. VPN, email, etc.
 - Bricks-to-clicks business that has opened their networks to do B2B, B2C & B2G business
- **All businesses using the internet**



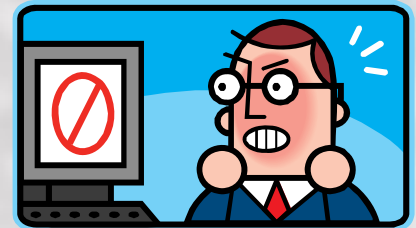
Technology Insurance Perils

- Virus
- Insider abuse of internet access
- Unauthorized access by unauthorized person
- Breach in security, hacking
- Theft of proprietary information
- Denial of service or access attacks
- Sabotage of data or networks
- Financial fraud
- Identity theft

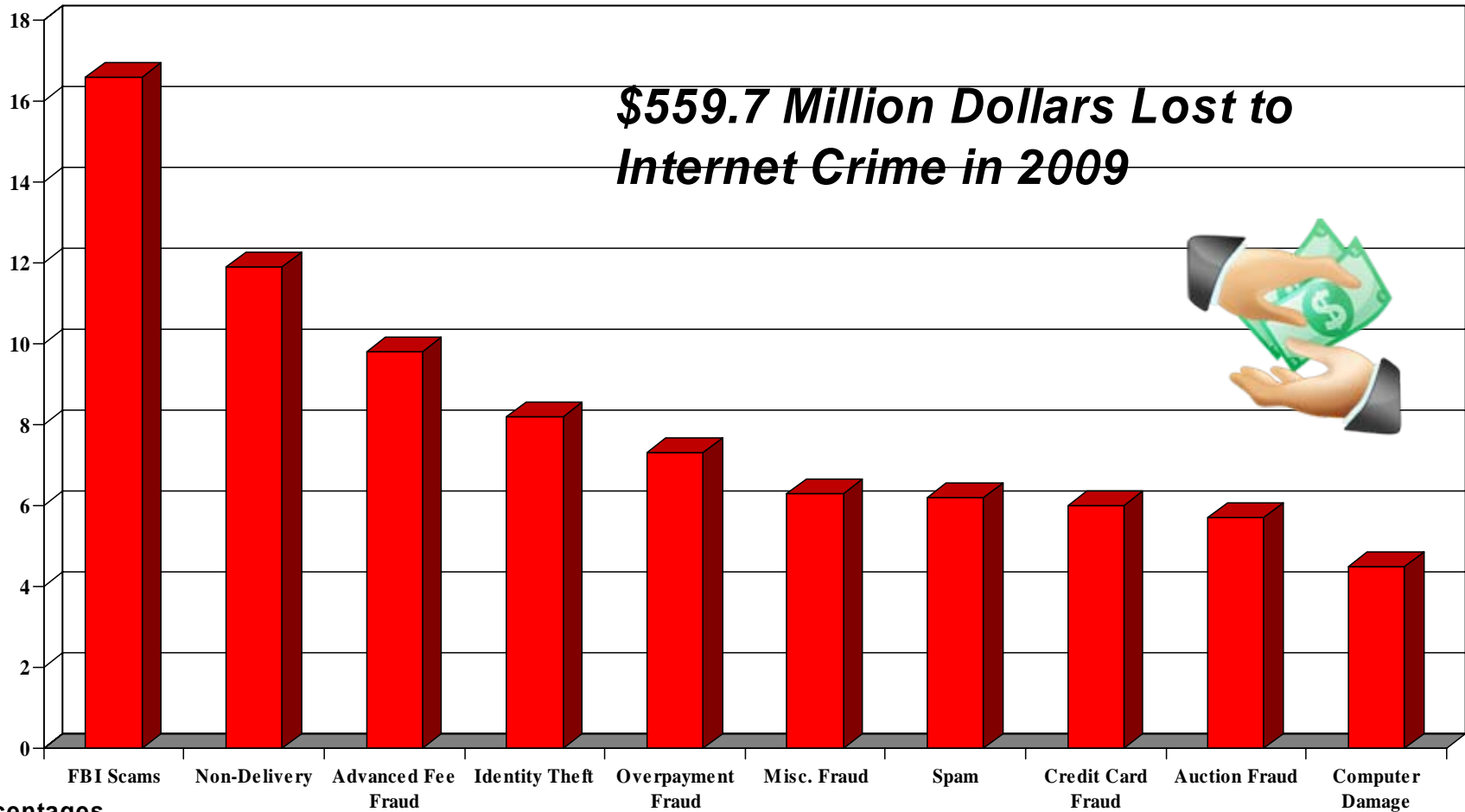


Computer Vulnerabilities

- Easily guessed passwords
- Not keeping secrets
- Untrained personnel with lack of security awareness
- Misadministration of systems
- Running trusted services over not trusted networks
- Trusting protocols that don't authenticate
- Trusting things (data, file, code) you get from others
- Downloaded software
- Stupid vendor tricks



2009 FBI Internet Crime Report



Security is not enough!

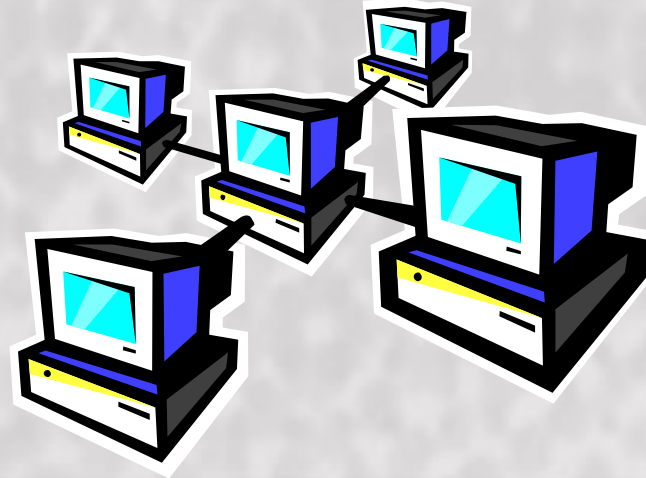
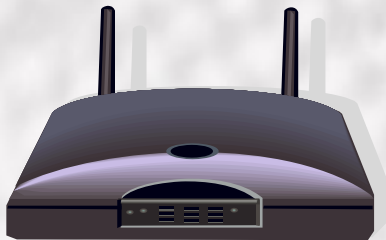
- Most businesses that suffer a technology or internet-related loss have anti-virus software and/or firewalls in place.



What is the probability it will happen to my organization?

- Losses experienced annually
 - 20% are experiencing 22 or more
 - 68% are experiencing 6 losses
 - 12% fewer than 2 losses

-According to IT Policy Compliance Group Feb. 2007



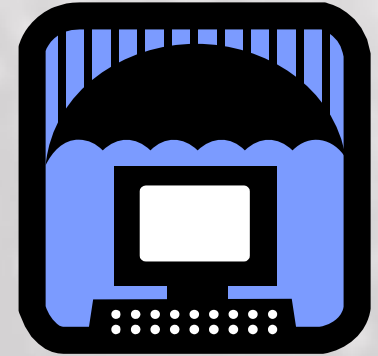
Benefits of Technology Insurance

- Protection against financial loss
- Your peace of mind
- Your customer's peace of mind
- Easing your customer's fear of doing business with you and over the internet



Assets That Need Protection

- Personal information (financial)
- Customer databases
- Customer credit information
- Company files and records (bank account)
- Intellectual property, patents and trade secrets
- Inventory, i.e. CDs, books, clothes, golf equipment, etc.



If you only learn one thing about the internet today, learn this:



A hacker in your network is the same as a robber in the physical world.



Third Party Coverage

- Defamation
- Infringement of right to privacy, breach of confidence (unauthorized collection or misuse, loss of data)
- Infringement of intellectual property rights
- Transmission of virus
- Denial of service
- Credit card injury
- Loss caused by breach of security



First Party Coverage

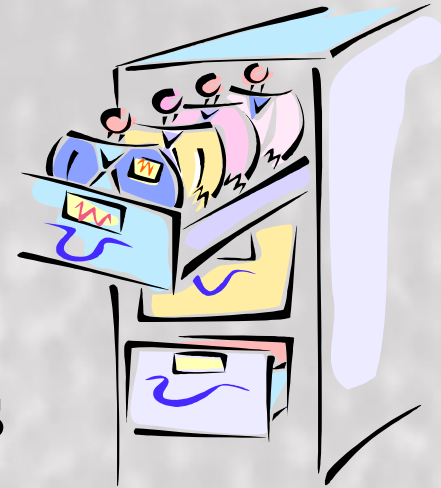
- Business interruption (breach of security, virus, denial of service)
- Property damage to electronic code
- Damage or loss to electronic data
- Enforcement of intellectual property rights
- Special benefits (investigation expenses, restoration costs, marketing and public relations expense)
- Extortion
- Fraud



Database Coverage

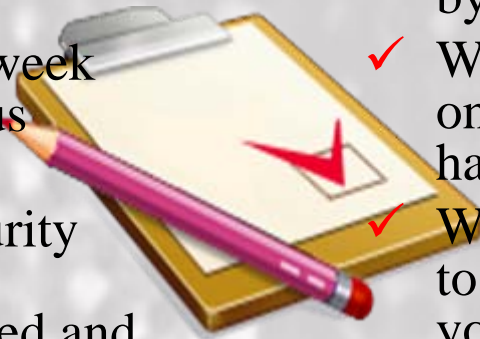


- Crisis management response
 - Stolen identity liability
 - Administrative expenses
- Providing service to customers



Risk Management Checklist

- ✓ Does your company use the internet for email?
- ✓ Does your company operate a website?
- ✓ Has it been more than one week since you updated your virus protection software?
- ✓ Is your corporate-wide security process implemented and communicated to newly hired and recently “unhired” employees?
- ✓ Are you relying on your hosting company to provide your website security?
- ✓ Has your company’s website ever been hacked?



- ✓ If your company’s website is hacked, will it take you more than 6 hours to be back in business?
- ✓ Are you relying on traditional insurance products for coverage if your website gets hacked by an external or internal hacker? If yes, by whom?
- ✓ Will your customers be the first ones to inform you that your website has been hacked?
- ✓ Would your customers be reluctant to use your website if they knew your website security had been breached?
- ✓ Would more than a 24-hour downtime of your website impact your bottom line?
- ✓ Does your company accept credit cards and store them in a database?

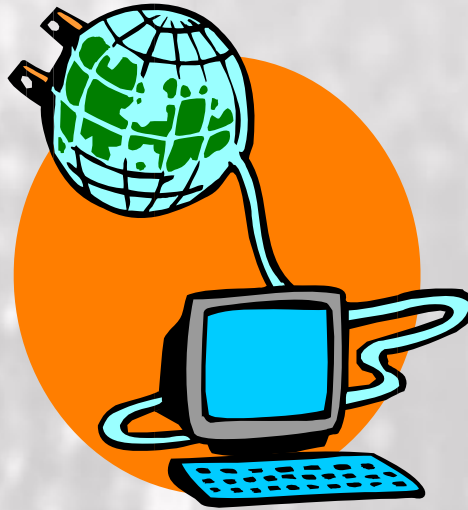


Three Truths of Insurance



1. Most companies hate paying insurance premiums until they have a claim
2. Purchasing insurance is not a high priority until you need it
3. If your company doesn't purchase insurance, then you have made the decision to assume all the risk by self-insuring





Call us today

to learn more about transferring your unwanted
Internet & Technology (Network) risks and
exposures.

