

Liability Implications of Security Vulnerabilities

Paul A. McNabb
Senior VP and CTO



An Eternal Truth

**“No man’s property is safe
as long as there is a legislature
meeting anywhere.”**

southern politician, 1838

Growing Set of Computer Security Laws

- ◆ **Counterfeit Access Device and Computer Fraud and Abuse Act of 1984**
 - ◆ First federal computer crime law, mostly concerned with access and classified information
- ◆ **Computer Fraud and Abuse Act of 1986**
 - ◆ Added crimes for computer fraud, damage of information, and trafficking in passwords (Robert T. Morris, Jr. was charged under this act)
- ◆ **Electronic Communications Privacy Act**
 - ◆ Defines privacy and monitoring rights

Liability and Negligence

Liability is imposed when there is either

- ◆ negligence
- ◆ intentional tort (usually criminal)

How does one show **negligence**?

- 1 show a **standard** or “duty of care” (“reasonable man”)
- 2 show a **breach** of that standard or duty
- 3 show proximate **causation**
- 4 show **damages**

Professional Negligence

- ◆ Held to a higher standard than just “reasonable man standard”
- ◆ Defendant must have taken “necessary precautions” to inhibit or prohibit damage
- ◆ Defendant must have acted “prudently”

Is “Standard Practice” Good Enough?

“In areas of changing technologies, where the potential harm is great, it is not unprecedented for courts to find negligence where the defendant has failed to implement security measures greater than those adopted by similar companies.”

Legal opinion, Lord, Bissell and Brook, 2000

T.J. Hooper, et al. v. Northern Barge Corp.

- ◆ in 1932, two barges were lost to a storm that arose after the tugboats had left port
- ◆ the tugboat company had followed standard business practice
- ◆ there was no law mandating radios and no industry standard that they be carried
- ◆ it was determined that if the boats had had a radio, the loss would not have occurred
- ◆ defendant was found liable for the loss

T.J. Hooper, et al. v. Northern Barge Corp.

“a whole calling may have unduly lagged in the adoption of new and available devices”

“there are precautions so imperative that even their universal disregard will not excuse their omission.”

Judge Learned Hand, 60 F.2d 737 (2nd Cir. 1932)

Is “Standard Practice” Good Enough?

“[courts] may determine that hacking or unauthorized access to systems by rogue employees is so grave and known a risk that the defendant institution should have implemented X, Y and Z security measures ... regardless of whether the industry is required to adopt or has generally adopted such technologies.” (emphasis added)

Legal opinion, Lord, Bissell and Brook, 2000

Is “Standard Practice” Good Enough?

“knowledge of weaknesses in various security measures may be attributed to a financial institution’s management, and stronger security practices adopted by other financial institutions would again provide a plaintiff with support for claiming that the defendant financial institution knew that its own systems were capable of penetration”

Legal opinion, Lord, Bissell and Brook, 2000

Systems Under Attack

As Network Use Grows, So Does Crime

In a 1999 Computer Security Institute/FBI study of 521 large organizations—including banks and government agencies—

- ◆ 62% of respondents had experienced security breaches over the past 12 months.
- ◆ 21% answered “don’t know”

-
- ◆ 91% utilize firewalls
 - ◆ 98% use anti-virus software
 - ◆ 93% deploy access control
 - ◆ 42% have intrusion detection

Systems Still Under Attack

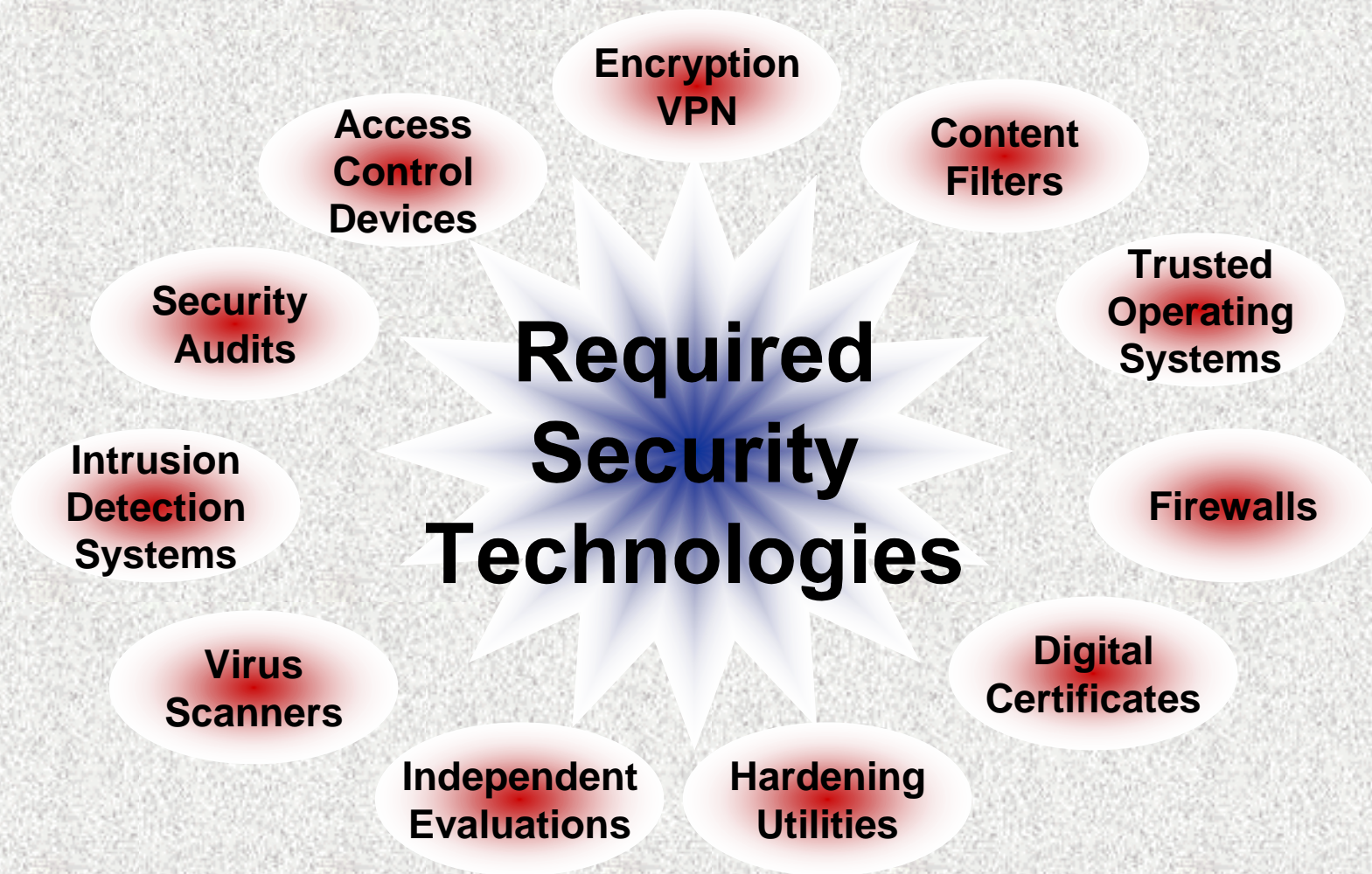
As Network Use Grows, So Does Crime

In a 2000 Computer Security Institute/FBI study of 643 large organizations—including banks and government agencies—

- ◆ 70% of respondents had experienced security breaches over the past 12 months.
- ◆ 12% answered “don’t know”

-
- ◆ 78% utilize firewalls
 - ◆ 100% use anti-virus software
 - ◆ 92% deploy access control
 - ◆ 50% have intrusion detection

What Technologies are Required?



Categories of Risk

◆ Transaction Risk

risk to earnings or capital arising from problems with service or product delivery

◆ Strategic Risk

risk to earnings or capital arising from adverse business decisions or improper implementation

◆ Reputation Risk

risk to customer and business relationships arising from adverse public opinion

◆ Compliance Risk

risk associated with non-compliance to laws, rules, regulations, prescribed practices, ethical standards

Businesses Under Attack



E-Commerce: Values at risk

◆ Asset Theft

- ◆ Money, Credit Cards, Intellectual Property
- ◆ CD Universe: theft, extortion, recovery cost (AmEx)
- ◆ ECommerce Times: indirect theft by Internet bank

◆ Privacy Disclosure

- ◆ Medical records (U of WA), credit ratings, customer database, R&D results, Patents

◆ Business Disruption

- ◆ eBay: \$4B in 22 hours

◆ Misinformation

- ◆ Public Image: CIA, FBI, NASA
- ◆ Stock market manipulation

Growing Damages

The 2000 CSI/FBI study of 643 corporations and agencies showed:

- ◆ **Total losses in 1999 and 2000 grew from \$124M to \$266M**
- ◆ **Theft of proprietary information and financial fraud cost went from \$83M to \$123M**
- ◆ **System penetration costs went from \$8M to \$28M.**

Bottom Line

- ◆ **What was legal yesterday could be illegal today.**
- ◆ **What is acceptable today could be unacceptable tomorrow.**
- ◆ **You could be liable even if you are following normal security practices.**
- ◆ **Attacks are growing and damages are increasing.**
- ◆ **There is very little case law to look to for help.**
- ◆ **Standards?**



Argus Systems

Securing the Future

For More Information



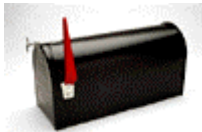
www.argus-systems.com



info@argus-systems.com



Tel: 217-355-6308
Fax: 217-355-1433



1809 Woodfield Drive
Savoy, IL 61874 USA