A Tale of Two Theories

Dennis Devlin
Assistant Vice President
Information Security and Compliance Services
The George Washington University
About the Topic

• Information security (data security) is not new and predates the Internet by decades
• Business was first to understand the value of protecting digital information as an asset
• Academia was first to understand the power of internetworking \( (\text{value} = f(\text{nodes} \times 2)) \)
• Each approached security very differently
• Those two approaches are now converging
About the Presenter

• Information Technology
  – 1972-1985 Hoechst (Aventis)
  – 1985-1996 Harvard University
  – 1996-1997 Independent Consultant

• Information Security
  – 1997-2007 VP/CSO Thomson (Thomson-Reuters)
  – 2007-2011 CISO Brandeis University
Business IT (c. 1976)

• IBM 370 mainframes
  – OS/VS, MVS, CICS, IMS
  – 3270 dumb terminals and controllers
• Coaxial hard wired network that did not leave the building or connected over leased lines
• Every user was a vetted, fellow employee
  – Focus on preventing errors and availability
  – Concept of safe inside and danger outside
Users Urged to Recognize Full Scope of Data Security

By Toni Wiseman
Of the CW Staff

CHICAGO – There are three important things to bear in mind when considering the protection of data, Robert Courtney, director of data security and privacy for IBM, told attendees at a Computer Protection/Insurance seminar here recently.

The first thing to realize is there is a wide variety of things which can happen to data; therefore, a broad definition of data security must be formulated, he said.

The realization that data is a major corporate asset is the second tenet, and, last but not least, the user must accept the need for a completely rational, feasible risk assessment technique, he said.

The lack of any one of these elements will result in an ineffective data security system, Courtney said.

Data security systems are intended to guard against accidental or intentional disclosure, modification or destruction of data, he said.

"If we are going to attack our data security problems in a systematic and rational way, we must prioritize our problems," Courtney outlined the six major data security hazards, with errors and omissions topping the list.

Dishonest employees and immediate past employees are the second most important hazard, he said. "It's a fact people rip off that part of the system they know best," Courtney said.

"They don't cross boundaries." This means an employee will generally abuse that part of the system he has already been granted entry to, so access control alone will not solve the problem. Rather, the solution is to be found in individual accountability, he said.

Third on the list of hazards is fire, Courtney said.

"Relatively few fires start in computers themselves," he said, "yet managers of DP facilities have a strong tendency to put fire-detection and fire-quenching equipment where the dollars are and not where the combustibles are."

Firms have an affinity for situating their computer rooms on top of cafeterias, usually right above the stoves, or under the cafeteria below the dishwashers, Courtney said.

Fire protection is important in areas where files, tapes and power sources are located as well as in the computer room since "even if your computer is still operating, it won't do you any good if your back-up files are gone or the communications lines are down."
Business Data Security (c. 1976)

“Things to bear in mind when considering the protection of data.”

1. There is a **wide variety of things that can happen** to data.
2. Data is a major **corporate asset**.
3. Users must accept the need for a completely rational, feasible **risk assessment** technique.

Robert Courtney (IBM)
Business Data Security (c. 1976)

The 6 major data security hazards:
1. Errors and omissions
2. Dishonest and past employees
3. Fire
4. Disgruntled employees
5. Broken water pipes
6. Strangers

Robert Courtney (IBM)
Business Data Security (c. 1976)

Definition

Data security systems are intended to guard against accidental or intentional disclosure, modification or destruction of data.

Robert Courtney (IBM)
Business Security Model

Them

Us
The Internet (c. 1985)
Academia IT (c. 1985)

- Sun, DEC, Apollo workstations and minis
  - BSD, System V, POSIX, VMS, network enabled OS’s
  - Apple Macs and IBM PCs

- ARPANET, BITNET, LANs, fiber backbones as interconnected as you could make them

- Every user a fellow early adopter of networks
  - Focus on connecting and sharing information
  - Little concept of inside vs. outside, risk or danger
Academia Security Model

Us
The Morris Worm (c. 1988)

• On November 2nd a new worm infected the ARPANET and hit 10% of the 88,000 hosts
• There were no managed demarcations between nodes on the ARPANET and the need for firewalls became rather apparent
• DARPA formed CERT at CMU as the first ever incident response team
• That was the only CERT Advisory in 1988
• In 1989 the ARPANET officially became the Internet and the rest as they say is history
The Internet (c. 2000)

Now You Are Here
Business Approach (c. 2000)

- Deny by default
- Allow by exception
- Network Address Translation (NAT)
- Enterprise “bastion” firewalls
- Company owned devices
- Company managed devices
- Security a condition of employment
- Network proxy visibility
- Web content filtering
Academia Approach (c. 2000)

- Allow by default
- Deny by exception
- Public IP addresses
- Device or LAN firewalls
- BYOD + Institution owned devices
- User managed devices
- Security as recommended practices
- Expectations of anonymity
- Unlimited network access
Security Approaches (c. 2000)

**Academia**
- Allow by default
- Deny by exception
- Public IP addresses
- Device or LAN firewalls
- BYOD + University
- User managed devices
- Recommended practices
- Expectations of anonymity
- Unlimited network access

**Business**
- Deny by default
- Allow by exception
- NAT
- Enterprise firewalls
- Co. owned devices
- Co. managed devices
- Conditions of employment
- Network proxy visibility
- Web content filtering
The Past Decade

• There is no longer a perimeter (80, 443, SOA)
  – Where do “we” end and “they” begin? (Jericho)
• Much of the data we process is now regulated
  – Not just reputation and revenues anymore (ROI)
• The consumerization of IT (DIY with credit card)
  – Cloud, BYOD, SAAS, “decustomerization”, …
• The weakest link continues to evolve and move
  – Server>network>application>browser>human>?
Irrefutable Laws of Information Security

1) Information wants to be free.
2) Code wants to be wrong.
3) Services want to be on.
4) Users want to click.
5) Even a security feature can be used for harm.

Malcolm Harkins (Intel)
Security Approach (c. 2010)

**Academia**
- Allow if possible
- Deny if necessary
- Public + NAT + move to IPv6
- Multiple zones + Starbucks
- BYOD + University
- Focus on data vs. device
- Policy + WIIFM
- Expectation of anonymity
- Unlimited access with ID

**Business**
- Deny if risky
- Allow if reasonable
- Public + NAT + move to IPv6
- Multiple zones + Starbucks
- Company + BYOD
- Focus on data vs. device
- Condition of employment
- Awareness of privacy laws
- Access that helps business
Measuring Risk Going Forward

• What regulated or sensitive data do you have?
• What adversaries want your data and why?
• What’s the value of data to your organization?
• How would your adversary value it?
• What are your adversary’s capabilities?
• What controls protect your information?
• Is your current level of risk acceptable?
Q&A

There is never enough time.
Thank you for yours.

Dennis Devlin
dmdevlin@gwu.edu