

Cyber 101:

Why is Cyber Security Important Now?

Patrick Faust
Chicago Board of Trade

Kenneth Newman
CISM



Disclaimer: Use perspective, and don't believe everything you hear...

Where are we?



- Ken

- Information Risk Management Department (ITRM)
- Director -> MD (Security technology and Monitoring)
- MD -> CIRO -> Div. CIO -> CITO
- Large, structured, centralized organization

- Patrick

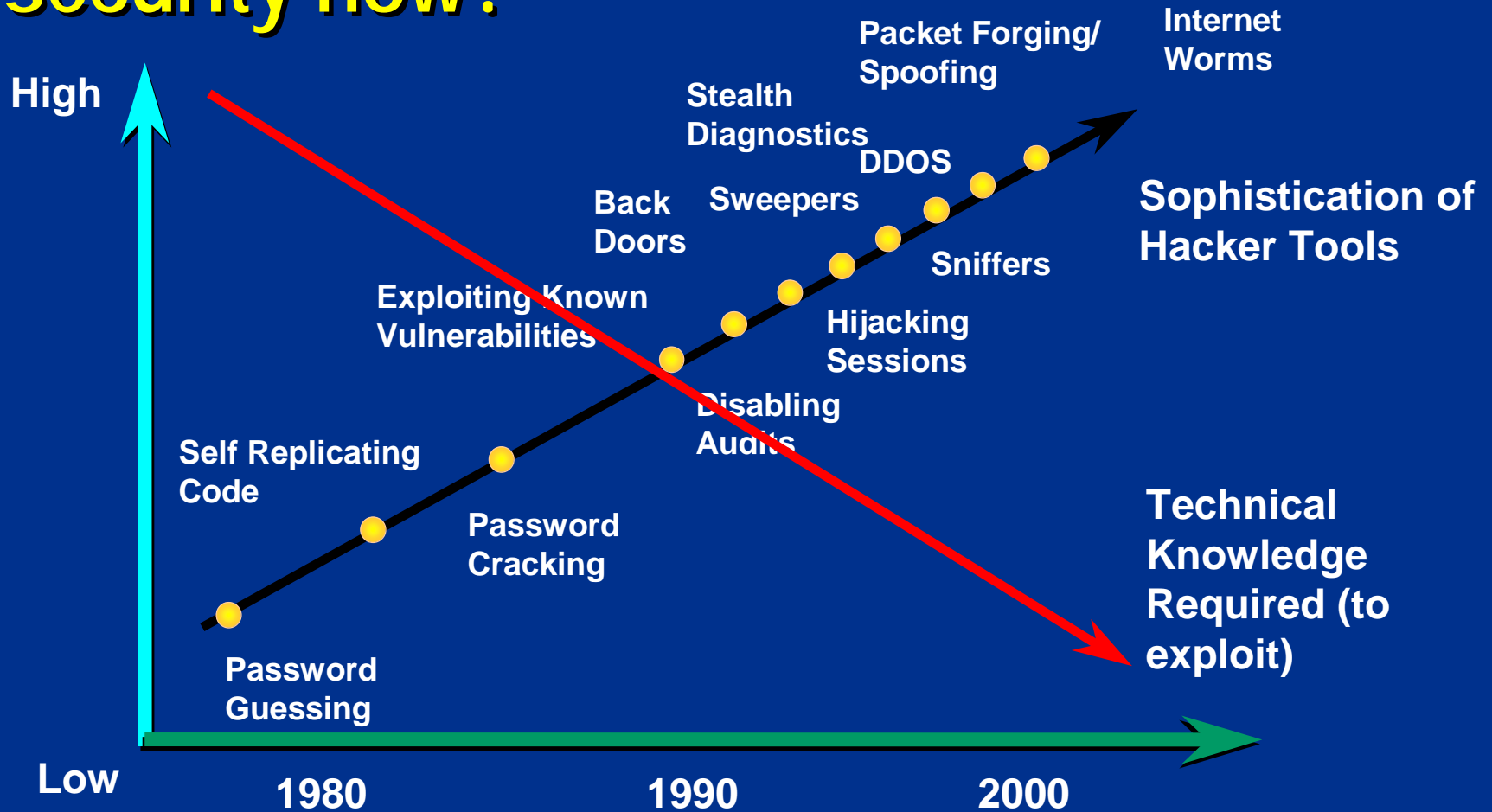
- Info Security and Business Continuity
- VP -> CIO (EVP) -> President
- Futures exchange (floor and electronic)

Why be concerned about cyber security now?



- “Scary stories”
 - More and more systems are automated
 - Realization: cyber threats potentially cause damages previously only associated with physical threats
 - Complacency: people are starting to expect problems
- Advances in the Technology
 - Convenience, cost, availability, & usefulness
 - Increased threats in type, number and complexity
 - Risks are outstripping protective safeguards

Why be concerned about cyber security now?



Graph: Cisco, Inc.

Why be concerned about cyber security now?



- Regulators
 - State of California privacy legislation SB 1386 (7/1/03)
 - Legal obligation to inform clients of breaches
 - SEC ‘SOX’ (6/15/04+) (Driven by Congress)
 - Ensuring financial statements are accurate
 - Of course, HIPAA, GLBA, and the Basel II Accord
 - Copyrights
 - DMCA (and litigation around music swapping)
- Internet & growth in e-commerce
 - Raise your hand if you haven’t heard this one yet!

Why be concerned about cyber security now?



- Telecommuting (Internet, telephone Dial-up connections)
 - B2B, B2C, suppliers, etc.
 - Employee/contractor remote users
 - Remote maintenance/ops controls (e.g. Energy Grid)
 - Desktop access through the web vs. traditional VPNs
- Digital Switch Telephony
 - Network based integration of voice and data
 - Attaching voice messages to data formats – e-mail, etc.

Why be concerned about cyber security now?



- Smart people (out of work) & cyber crime pays
 - Social Engineering (weakest link)
 - The Art of Deception, Mitnick
 - Corporate espionage
 - Staff anxiety (downsizing, etc.)
 - Script kiddies
 - Outsourcer's outsourcer?
 - Hackers vs. crackers
 - Socio-political hacktivism
 - Terrorism
 - Identity theft (to cover a criminal's tracks)
 - Cheaper, less experienced staff guarding the gates



Why be concerned about cyber security now?



- Data retention
 - Legal requirements
 - Maintaining controls on backups
- Disposal of information and equipment
 - Discarded/donated computers (a data gold mine)
 - Dumpster diving
- Outsourcing
 - Internal operations and staff? Not anymore!
 - ‘Offshore’ countries’ control capabilities?
 - Your perimeter is crumbling as you extend it...

Why be concerned about cyber security now?



- Mobile and wireless technology
 - Smart phones/blackberries – e-mail/file forwarding
 - Cell phones/pagers - SMS text messaging
- WI-FI
 - An access point from Best Buy vs. your security model
 - Your laptops reaching stronger external access points
 - Like most products, Wi-Fi security is disabled by default
- Personal Electronic Devices
 - Portable devices - PDAs, USB tokens, etc.
 - Another data gold mine if lost or stolen

Why be concerned about cyber security now?



- Pervasive technology
 - Web-based e-mail (Hotmail, etc.) & instant messaging
 - P2P file sharing (bandwidth, storage, and legal issues)
 - Unsanctioned/unmonitored forms of communication
- Virii, worms, and trojans
 - Challenge of patch/configuration management
 - Decreasing time from vulnerability -> exploit -> “wild”
 - We haven’t yet seen truly malicious payloads
 - More sophisticated trojans ‘mimic’ user activity
 - Virii/worms can inject trojans (and so can spoofed sites)

Why Worry About Cyber Security?



- Various Types of Risk Exposure
 - Confidentiality, integrity, availability, etc.
 - Individual impact based on probability and likelihood
 - Depends on your perspective of a given environment
- Examples: Biggest Fears (other than cost):
 - CEO: lost reputation/market confidence = lost business
 - Legal department: regulatory sanctions, legal exposure
 - Operations: frequency and duration of downtime
 - Human resources: privacy protection
 - Security/risk management: It's all our job

SECURITY=TRUST=BRAND

Keys to Selling Senior Mgmt / Business Mgmt



- FUD Factor (Fear, Uncertainty, and Doubt)
 - Shock is not sustainable or helpful in long run
 - Not career enhancing (chicken little never got ‘ahead’)
 - “Accidental Fall Guys” (infosec may be on the hook)
- Relate to risk management
 - Conceptually like credit or market risk
 - Language the business understands
 - ROI and cost/benefit analysis
 - Industry benchmarks and standards - Basel, etc.
- Focus on process and not on point products

Keys to Selling Senior Mgmt / Business Mgmt



- Risk Assessments (external/internal reviews)
 - Establish/evaluate policies (acceptable use policy 1st)
 - Surveys & inspections
 - Analysis of vulnerabilities
 - Process review
 - List/rank vulnerabilities
 - Risk Mitigation
 - Cost/benefit analysis
 - Appropriate controls to protect information
 - Establish annual benchmarks & objectives
 - Education & awareness of entire process



Information Security Jargon Execs should Know



- Some key terms

- Risk Assessment
- Risk Management Committee
- Risk Acceptance Letter
- VPN
- Firewalls
- IDS
- User Identity Management
- Insider Threat
- Strong (2 factor) Authentication
- encryption
- IPS
- SOX
- HIPAA
- GLBA
- Basel
- DMCA
- SB 1836
- Wi-Fi (802.11)
- CIA
- Incident Response
- Patch Management
- Malware

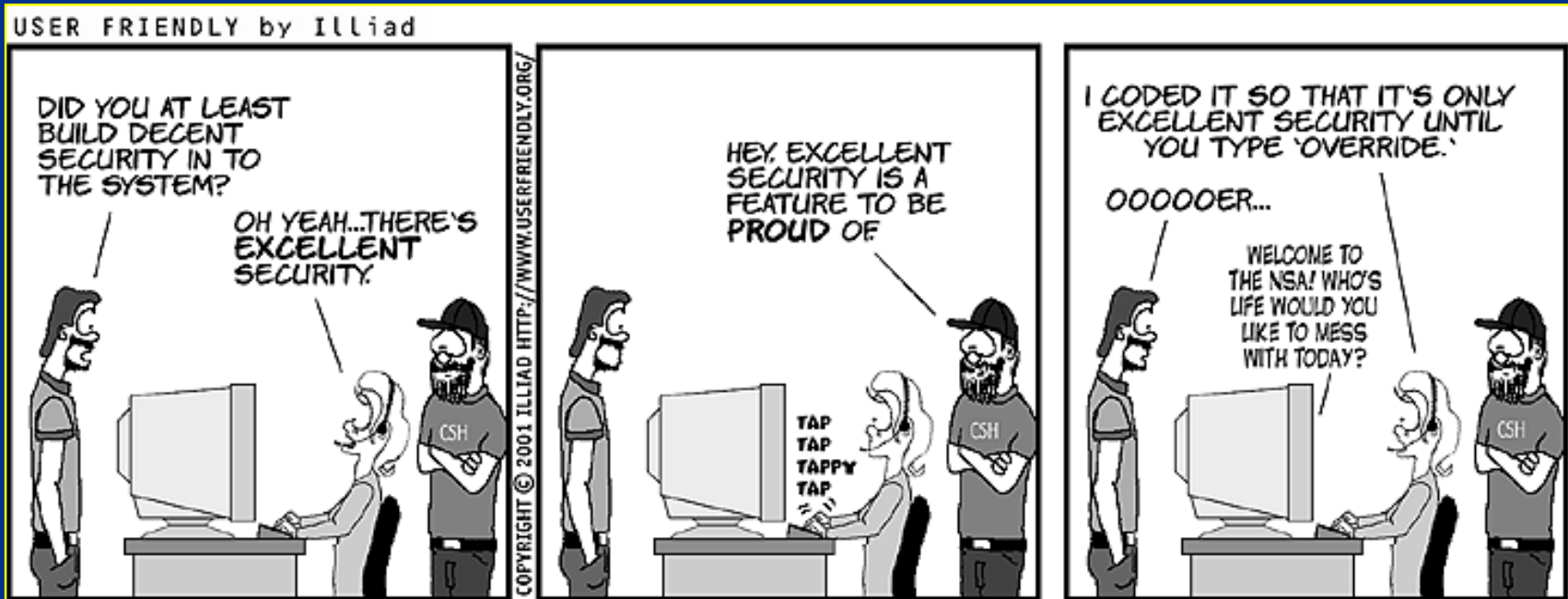
Information Security Jargon Execs should Know



- URLs

- www.searchsecurity.com
- www.consumer.gov/idtheft
- <http://www.sec.gov/about/laws.shtml#sox2002>
- <http://www.loc.gov/copyright/legislation/dmca.pdf>
- www.hipaa.org
- <http://www.bis.org/bcbs/>
- <http://www.epic.org/privacy/glba/>
- <http://www.new-technologies.com/ntsec/statutes.htm>
- <http://www.rspa.com/spi/project-risk.html>

Questions?



Patrick Faust, Chicago Board of Trade

pfau44@cbot.com

Kenneth H. Newman, CISM

khn15@columbia.edu