You Cannot Manage, What you Cannot Measure: Security Risk Metrics

State of CA CISO Lecture Series

Stuart McClure
VP Operations/Strategy
Risk and Compliance Business Unit
McAfee, Inc.
How to motivate change...
Carrot? Stick? ...Both?

1. **Attack** (worm, malware, privacy breach)
2. **Compliance Deadlines** (FISMA, IAVA, PCI)
3. **Live Demonstrations** (approved on your own systems, databases, accounts of course!)
4. **Security Metrics** (Quantify and track your risk over time. Predict your next attack/breach…)

In the end... It’s all about relationships, building trust and credibility…
Agenda

• Security Drivers
• Security Metrics
• Real World Examples
Security Drivers
What drives us?
*Threats: Opportunity Meets Motivation Meets Ability...*

- Bots, Botnets, DDOS networks
- Spam, mass-mailers, phishing, pharming
- Targeted attacks
- Spyware, Adware, PUPs
- PDA, cell phone, wireless
- User-propagated viruses, Trojans, PW stealers
- Vulnerabilities, Exploits, Scripted attacks
- Social Engineering
Misused Functionality – In the Real World…

- April 19, 1995
- 168 souls
- Commonly used materials costing $5,000
• Famous examples:
  – Mass mailing functions
    • Melissa virus (1999)
    • ILOVEYOU (2000)
  – ActiveX functions
    • Zlob Trojan (2005)
  – Icon modification functions
    • OSX/Leap (2006)
  – Autorun/Autoplay functions
    • W32/Virut (2003)
    • W32/Sality (2006)
    • Autorun.worm.gen (2008)
  – IE’s Browser Helper Objects (BHO)
    • PWS.Cashgrabber (2005)
    • PWS.Banker (2008)
  – File sharing
    • Conficker.B (2009)

Mitre recently added new category – Common Configuration Enumeration (CCE)
Misused Functionality – In the Security World…

Autorun: The Floppy Disk of the New Millennium
Design Flaws – In the Real World…

- Feb. 24, 1989
- 9 souls
- Faulty cargo door design
- Went unfixed for years
• Famous examples:
  – MS01-033 (Code Red) – 2001 (1 mo)
  – MS02-039 (SQL Slammer) – 2003 (6 mos)
  – MS08-067 (Conficker) – 2008 (2 weeks)
• SANS reports 60% of attacks today are web based
• CVE rate = 18/day, 3700 average/yr
• Over 39,000 vulns in NVD. Over 40,000 in CVE:
Malicious Intent

- War Games movie (1983) [Matthew Broderick]
- Moonlight Maze (1998-99)
- “Good Times” virus (1994)
- First Word Macro viruses (1995)
- Solar Sunrise (1998) [Ehud Tenenbaum]
- Melissa virus (1999) [David L. Smith]
- ILOVEYOU virus [Reomel Lamores], DDOS attacks (2000)
- Rbot/Sdbot/Zotob (2005) [Farid Essebar aka “Diabl0” and Atilla Ekici aka “Coder”]
- Storm Worm (2007)
- TJX/Heartland/Hannaford, etc. (2009) [Albert Gonzalez]
Making it Real – Recent News…

- Three hackers indicted in NJ on 8/17/09
  - 1 co-conspirator not indicted
- Allegedly responsible for:
  - T.J. Maxx (94M), Heartland (130M), Hannaford Bros. (4.2M), 7-Eleven, Barnes & Noble, BJ’s Wholesale Club, Boston Market, DSW (1.5M), Forever 21 (99k), Office Max (200k), Sports Authority
- Attacked from systems/zombies from:
  - US (NJ/CA/IL), Netherlands, Ukraine, Latvia
- Techniques used:
  - SQL Injection attacks
  - Installed malware (including AV bypassing)
- References:
  - [http://voices.washingtonpost.com/securityfix/heartlandIndictment.pdf](http://voices.washingtonpost.com/securityfix/heartlandIndictment.pdf)
Cyber Crime Ecosystem (The Bad Guys)

CYBERCRIME IS EVOLVING

- End Users = Data
- Identity Thieves
- Spammers
- Tool Developers
- BOT Herder
- Vulnerability Discoverers
- Malware Developers

011010010001
Malicious Intent: The result - Malware YTD

- 200,000 unique malware per month
- 6,000 per day

More than double last year’s midyear metric
Security Metrics
Risk and Compliance

The Dilemma

**Increasing Risk**
- Threats
- Vulnerabilities
- Change
- Regulations

**Decreasing Protection**
- Insufficient budget
- Limited people resources

**Result: Controlled Chaos**
- Lost data / Privacy breaches
- Decreased system availability
- Poor system performance
- Configuration creep
- Audit/Remediate/Repeat
- Reactive fire-fighting
- Delays in strategic projects
- Lost business
1. Reduce time and cost associated with patching and audits
2. Manage more effectively against policies
3. Report-on-demand for internal or external audits
4. Increase security of my data, applications, and network
5. Enhance system availability and application performance

Get in Control, Stay in Control
Risk and Compliance

Assess Completely
Remediate Easily
Enforce Automatically
Optimize Security
Report Intelligently

Get in Control
Stay in Control

“Audit Once, Report Many”

Increased security and compliance
Enhanced availability and system performance
Reduced time & cost of audits, patching, upgrades
Compliance ≠ Security

Lessons learned...

CardSystems Solutions Inc.
Affected: 40M CCN
Lawsuit: Multiple
PCI: Event occurred before PCI
Source: Hacked

Hannaford Bros. Breached
Affected: 4.2M CCN w/exp dates
Lawsuit: March/April 2008
Source: Hacked, installed malware
Note: July 08 – CIO resigns

RBS WorldPay Breached
Affected: 1.5CCN / 1.1M SSN
Lawsuit: 2/18/09
Source: Hacked
Note: $9M in fraud

Heartland Payment Systems Breached
Affected: Unknown (est. 5-100M)
Lawsuit: Jan 28, 09 (NJ) – Class Action
Source: Hacked, installed sniffer malware

CardSystems Solutions goes Bankrupt

2005 2006 2008 2009

Heartland PCI Compliant By Trustwave
RBS WorldPay PCI Compliant By Trustwave
Hannaford Bros. PCI Compliant By Rapid7

Datalossdb.org
Managing Security Risk
Where do we start?

1. **Policy**
   Establish process, standards and guidelines

2. **Inventory**
   Discover all assets across the network

3. **Prioritize**
   Assign business value to assets

4. **Vulnerabilities**
   Determine vulnerabilities on assets

5. **Threats**
   View potential threats

6. **Risk**
   Determine risk level
   \[ R = \frac{A}{C} \times \frac{V}{C} \times \frac{T}{C} \]

7. **Block**
   Stop intrusions in real-time

8. **Remediation**
   Proactively fix vulnerabilities

9. **Measure**
   Proactively measure impact of security decisions and actions

10. **Compliance**
    Review for policy compliance
The relationship to cost and security and compliance diverge during progression to the managed and optimized states.

- Maturity of process reduces audits from months to days and enables sustainable compliance
- Cost savings occur through reduction of point products and increased automation
Key Customer Challenges
“Audit Fatigue” requires Automation

“Majority of IT Audit Controls are Manual”

57% of large organizations have automated less than 25% of their controls

Collecting accurate, timely data is a protracted effort. Difficult to ensure integrity of data.

*McAfee- commissioned IT Audit Study: Based on 400 IT audit-related professionals in North America and Europe (ISSA and ISACA). Conducted by the Internet Research Group*
Key Customer Challenges
“Patch Panic” creates delays in mitigation

“Anxiety inhibits action”

Symptom
– No definitive answer to: “Does the new threat released today apply to us?”

Statistics
– 5443 vulnerabilities added to NVD database in 2008

Consequences
– Distracts from day-to-day operational workload
– Decreases performance and availability of IT assets
– Exposes a lack of IT leadership and planning
Managing Security Risk
How do companies manage it?

- **Risk Transfer**
  - Contractual transfer to 3rd party or insurance provider.

- **Risk Avoidance**
  - The “power button” technique of risk management.

- **Risk Acceptance**
  - Cannot eliminate all risk, at some point someone/somewhere must accept what remains.

- **Risk Mitigation**
  - Find and apply security countermeasures (people/process/technology)
• **Qualitative**
  – Traditional IT audits (EY/PWC/DT) – SAS70/BS7799/ISO17799/ISO27001/ISO27002
  – Question/answers
  – “Checklist” jockeys/bunnies

• **Quantitative**
  – Independently verifiable
  – Objective
  – Repeatable
  – Automatable with technology
Are you spending your security dollars *the right way*?
What kind of return are you getting for your security dollars?
• Common Vulnerability Scoring System (0-10)
  – CVSSv2 (2007)
  – www.first.org/cvss
  – Scoring Components (3 major):
    • **Base Metrics**
      – **Exploitability Metrics**
        » Access Vector
        » Access Complexity
        » Authentication
      – **Impact Metrics**
        » Confidentiality Impact
        » Integrity Impact
        » Availability Impact
    • **Temporal Metrics**
      – Exploitability
      – Remediation Level
      – Report Confidence
    • **Environmental Metrics**
      • Collateral Damage Potential
      • Target Distribution
      • Security Requirements
• NVD CVSS online calculator
• Consensus Metric Definitions v1.0.0 (May 2009)
  – www.cisecurity.org
  – 20 metric definitions involving:
    • Incident Management
    • Vulnerability Management
    • Patch Management
    • Application Security
    • Configuration Management
    • Financial Metrics
  – First realistic security metrics program
  – More complex but more complete…
Quantitative Metrics
Foster Trust and Credibility…

Measure the “Major 3”:

1. Risk Rating (1-100)
   - Attack surface
   - Misused functionality
   - Design flaws
   - WoE
   - User awareness

2. Incident costs ($$)
   - Incident expense, loss time quantification, fines/lawsuits associated, notification costs

3. Security expense/spending ($$)
   - Operating expenses, Capital expenses

“.. Notification costs per data record are now $202…”
Quantitative Metrics - Risk Rating

• Attack Surface:

How many of you know exactly what assets you have and where you have them?

Q: How do you measure attack surface?

A: Find and track over time the number of devices on your network:
  • IPv4/IPv6: ICMP, TCP, UDP discover
  • IPX/SNA/APPC/AppleTalk
  • Query all asset databases, CMDBs, in realtime and on-demand
• Misused Functionality

*What configuration settings are present in your environment that contribute to exploitation and malware?*

*Q: How do we measure the number of functions present that can be misused?*

*A: Scan and track over time all your systems for the top 10 configuration weaknesses:*  
- Autorun enabled  
- File sharing enabled  
- Execution permissions on IE Temporary Folders  
- Etc…
What vulnerabilities are present in your environment that contribute to exploitation and malware?

Q: How do we measure the number of vulnerabilities present that can be misused?

A: Scan all your systems for at least the following:

- Microsoft Security Bulletins
- SANS Top 20 or similar
- OWASP Top 10 and/or CWE 25 (Web)
Quantitative Metrics - Risk Rating

• Window of Exposure (WoE)

How quickly does IT fix the problems that security finds?

Q: How do we measure your IT staff’s ability to patch and remediate the misused functionality and design flaws found?

A: Measure it with technology:

- Vulnerability Management program
- Patch Management program
- Configuration Management program
- Find the mis-configurations and vulnerabilities and measure how quickly they are remediated.
• User Awareness

*How educated are your users on general security hygiene?*

Q: *How do we measure your user’s preventative awareness?*

A: *Ask them (questionnaire - ideally at login):*

- Pick 5 to 10 questions about general user decision making skills:
  1. If you receive an attachment or a web link from someone you don’t know, do you open it?
  2. If you are given a USB key, do you plug it into your computer without scanning it?
  3. Do you go to websites you do not know are safe?
  4. Etc…
Design Flaws – Return on Investment

SDLC

• Microsoft’s Software Development Lifecycle (SDL)

![SDLC Diagram]

• Reduce the number of vulnerabilities

• Reduce the overall development costs

• NIST, May 2002 – eliminating vulnerabilities in design can cost 30x less than fixing them after release.

• Microsoft ROI whitepaper:  [http://go.microsoft.com/?linkid=9684360](http://go.microsoft.com/?linkid=9684360)
Behavioral Analysis
Applied to Security…

Motivation + Opportunity + Ability = Potential

**Motivation**
- Value of data available
- Laxed or non-existent laws
- Ease or difficulty catching

**Opportunity**
- Number of interconnected devices
- Number of vulnerabilities
- Number of functions available to misuse
- Sophistication of users/admins
- Number of tools available
- Number of domain registrations
- Number of websites accessible

**Ability**
- Knowledge level of the bad guys
- Criminal mentality
- Information publicly available
Conclusion

• Threats and events continue to increase
• Stay abreast with current world events
• Understand the current economic climate
• Understand your organization’s needs
• Measure EVERYTHING!

Thank you!

stuart_mcclure@mcafee.com
949-297-5585