Northwestern University
Network Security

Security Automation & Policy
Topics for Discussion

• IT Security in the Business
  – Risk, Audit Support, Compliance

• Policies, Standards, and Procedures
  – IT Security’s Role in Creation and Enforcement

• Security Automation
  – Reality of Security in the IT World
  – Explanation of the problem
  – Offense VS Defense (tools and stats)
The CISO Agenda

Business

- Managing 3rd Party Risk (Outsourcers)
- Executive / Board Reporting
- Privacy / Security Breach
- Brand Protection & Enhancement
- Alignment with Business Goals / Objectives

CISO

- Metrics / Benchmarking
- Disaster Recovery
- Linkage to Enterprise Risk Mgmt
- Identity Management
- Comprehensive

Technology Enablement

- Mobile Computing
- Evolving Threats
- Staffing Support
- Vulnerability / Patch Management
- Compliance / Internal Audit

Core Functions

- Strategy
- High Availability
- M&A
- Culture / Awareness
- Business Continuity
- Vulnerability / Patch Management
- Evolving Threats
Risk

IT Security performs a critical role in assessing risk in the organization.

- Vulnerability Scanning
- Penetration Testing
- Industry Trends
- IT Strategy
- Familiarity with Audit and Compliance measures
Audit Support

In many cases, IT Security is heavily relied upon to perform in depth testing required by an audit organization. Security is enlisted by audit because:

• Technical expertise
• Familiarity with current issues from internal testing
• Familiarity with Policies, Standards, and Procedures
Compliance

Compliance may relate to internal compliance or external compliance.

Internal compliance:
- Policies and Standards
- Security and Configuration baselines
- Framework use – ISO, COBIT, ITIL, GAISP, NIST
- Best Practices
Compliance cont’d

External compliance:
• SOX (Sarbanes Oxley)
  – COSO Framework
• HIPAA
• PCI
• Safe Harbor
# ISO Leading Practices

<table>
<thead>
<tr>
<th>ISO 27002 Best Practice</th>
<th>NIST</th>
<th>PCI DSS</th>
<th>SOX</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Risk Assessment and Treatment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5. Security Policy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6. Organization of Information Security</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>7. Asset Management</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8. Human Resources Management</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>9. Physical and Environmental Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10. Communications and Operations Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>11. Access Control</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>12. Information Systems Acquisition, Development and Maintenance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>13. Information Security Incident Management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>15. Compliance</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Compliance in Action

Cardholder Data
Financial Data
Personally Identifiable Information
Intellectual Property

ISO 27002
Other Control Frameworks (CoBIT, COSO, PCI DSS)

Authentication
Access Control
Logging
Encryption
Other Policies, Procedures, & Technologies

PCI DSS
Sarbanes-Oxley
Internal Policy
EU Data Protection

Identify Sensitive Data Types
Build a framework of leading practices based on ISO 27002
Discovering data and assessing existing controls across the framework
Apply controls consistently and repeatedly across the compliance areas
Internal Policy

IT Security is regularly tasked with creation and enforcement of IT policies, standards, and procedures. Creation and enforcement of these documents require:

• Understanding of audit roles and procedures
• Familiarity with all systems, networks, and applications
• Compliance considerations
Definitions:

• A **Policy** is a set of directional statements and requirements aiming to protect corporate values, assets and intelligence. Policies serve as the foundation for related standards, procedures and guidelines.

• A **Standard** is a set of practices and benchmarks employed to comply with the requirements set forth in policies. A standard should always be a derivation of a policy, as it is the second step in the process of a company’s policy propagation.

• A **Procedure** is a set of step-by-step instructions for implementing policy requirements and executing standard practices.
Internal Policy cont’d
Internal Policy cont’d

Policy creation and enforcement cycle

1. Creation
2. Approval/Application to Organization
3. Audit Performed
4. Report Findings
5. Create Mitigation Plan
Policy Business Case

A top 5 global food retailer has a massive IT/IS infrastructure and good governance....but no real policies!

Policies are the foundation for enforcing IT compliance and governance.

What policies were written for the client...
Policies written for IT Security:
• Acceptable Use Policy
• Information Classification & Ownership Policy
• Risk Assessment & Mitigation Policy
• Access Control Policy
• Network Configuration and Communication Policy
• Remote Access Policy
• Business Continuity Policy
• Incident Response Policy
• Third Party Data Sharing Policy
• System Implementation & Maintenance
• Secure Application Development
• Cryptography & Key Management
• Mobile Computing
• Physical & Environmental Security
Policy Business Case cont’d

Sample Policies
Translation to the Real World

Security policy can be written but is it applied??
The reality of IT security

90% of Companies say they have been breached in the last 12 months*

Billions of $$ in IT security spending

*Perceptions About Network Security, Ponemon Institute, June 2011
Attacks are increasingly publicized

Advanced Persistent Threat (Aurora, Sony, FBI, Google, RSA, L3)

Anonymous/LulzSec (HBGary, Sony, FBI)

Cyber-Criminals (Spy Eye, Zeus)
Why can’t we stop them?

• Verizon has studied recent breaches

• 92% of attacks were not highly difficult

• 96% of attacks could have been avoided
  – Better yet, they found it just takes “consistent application of simple or intermediate controls”

• How can that be?
The paradox

Let’s review:

1. Bad guys are getting in
2. We’re spending billions
3. Simple controls work

What’s going wrong?
Complexity is the enemy

• Verizon said “consistent” controls
  – In real networks, that’s hard
  – Complexity defeats us
• Humans don’t handle complexity well
• We set policy well
• Human effort just doesn’t scale
  – Too many details
  – Too many interactions
• Just how complex are real world infrastructures?
Here’s one real corporate network
Zooming in a bit...
Here’s one “doorway” into the network
One small typo created a problem

Where can you go from here?

One device with a single letter typo here
Implications of simple typo

Technical details:

- ACL as written:

```plaintext
ip access-list extended ACL-S61-534
  permit ip any <8 servers>
  permit ip any <8 more servers>
  permit ip any host <1 server>
  permit ip any host <1 more server>
```

- ACL as applied:

```plaintext
interface serial 6/1.534
  description Link To <outsiders>
  ip access-group ACL-61-534 in
```

- The access group lacks an S!

In English:

- **Good security rule, applied badly**
  - Hard for a human to spot
- **Expected access: extremely limited**
- **Actual access: wide open to a competitor/partner**
Casualties of complexity abound

**Financial Services**
Before Automation: Brand new data center, emphasis on increased security
With Automation: Found error in 1 firewall of 8 that destroyed segmentation

**Retail**
**Before Automation:** Believed they had enterprise-wide scan coverage
**With Automation:** Identified major gap – firewall blocked scanning of DMZ

**Bank**
**Before Automation:** Built segmentation between development and 401(k) zones
**With Automation:** Found addresses added to development had full 401(k) access
Another complex arena: chess

• Who’s better at chess?
  – Computers or humans?
• Kasparov now says “wrong question!”
• Ask how to play the best chess
  – Answer? Human-computer teams
  – He calls this “Advanced Chess”
• Humans are great at strategy
  – Weak on details
• Computers excel at exhaustive analysis

Advanced Security requires the same approach
The need for proactive security intelligence

- Objectives:
  - Cost-effective security
  - Avoid incidents
  - Pass audits
- Need “Kasparov’s chess computer”
- Continuously assess defenses
  - End to end, across the entire network
- Show the state of your network security
- Demonstrate compliance with network security policy
- Identify gaps and prioritize remediation based on risk
Recap Issues

• True security is about People, Process, and Technology
• Application of simple controls (policy) is required for compliance AND success
• Security is a “Big Data” problem
• Without automation to reduce complexity, security remains a dream
Both Sides of the Coin

Defensive:
  • There are not many tools to help the defenders protect all the doorways

Offensive:
  • There are a LOT of automated tools to help offenders find and break through those doorways
Let’s look at some poll results of the real world of security:
Options

Defensive Options:

Offensive:

<< back | track-linux.org
Backtrack

• Backtrack is a Linux based hacking toolkit provided by the people at [www.backtrack-linux.com](http://www.backtrack-linux.com)

• It includes a massive amount of hacking tools all for free 😊

• Compile tools yourself? Maybe check this out instead.
Backtrack

• Tool categories in BT4:
  – Digital Forensics
  – Information Gathering
  – Access Maintenance
  – Network Mapping
  – Penetration
  – Privilege Escalation
  – Radio Network Analysis (Wireless)
  – Reverse Engineering
  – VOIP
  – Vulnerability Identification
  – Web Applications
  – Miscellaneous
Backtrack

• Backtrack Demo
Backtrack

• Ways to use backtrack
  – Live CD: The most popular method
    • No state save
    • Highly portable
  – USB Drive/Stick
    • Highly portable (more so than CD)
    • Can make stateful
    • Prone to loss
  – Full HD install
    • Using your machine as a “hacktop”
    • Dual boot
  – Virtual Machine
    • Networking gets tricky
    • Resource availability
RedSeal Networks

• Visualize
  – End to end infrastructure

• Comply
  – Test network controls

• Protect
  – Actionable remediation

Automated & continuous
Three key questions

- Network Configs
- Host Scans
- Security Policies

RedSeal

- Continuous
- Comprehensive
- Automatic

- Visualize security status
- Comply with policy
- Improve protection

- Technology to answer:
  1. Where are your high risk vulnerabilities?
  2. Am I compliant with network security policy?
  3. How are IT changes impacting my security over time?
Visualize your network security

Immediately understand security posture

Communicate return on security investments

Detect anomalies & patterns
Continuously **comply** with policy

- Continuously monitor network for compliance

- Enforce industry recommended & custom configuration best practices

- Demonstrate compliance to auditors
Protect yourself from compromise

Highlight gaps in security
Identify high-risk vulnerabilities

Pin-point rules violating network policy

Assess risk of planned network changes