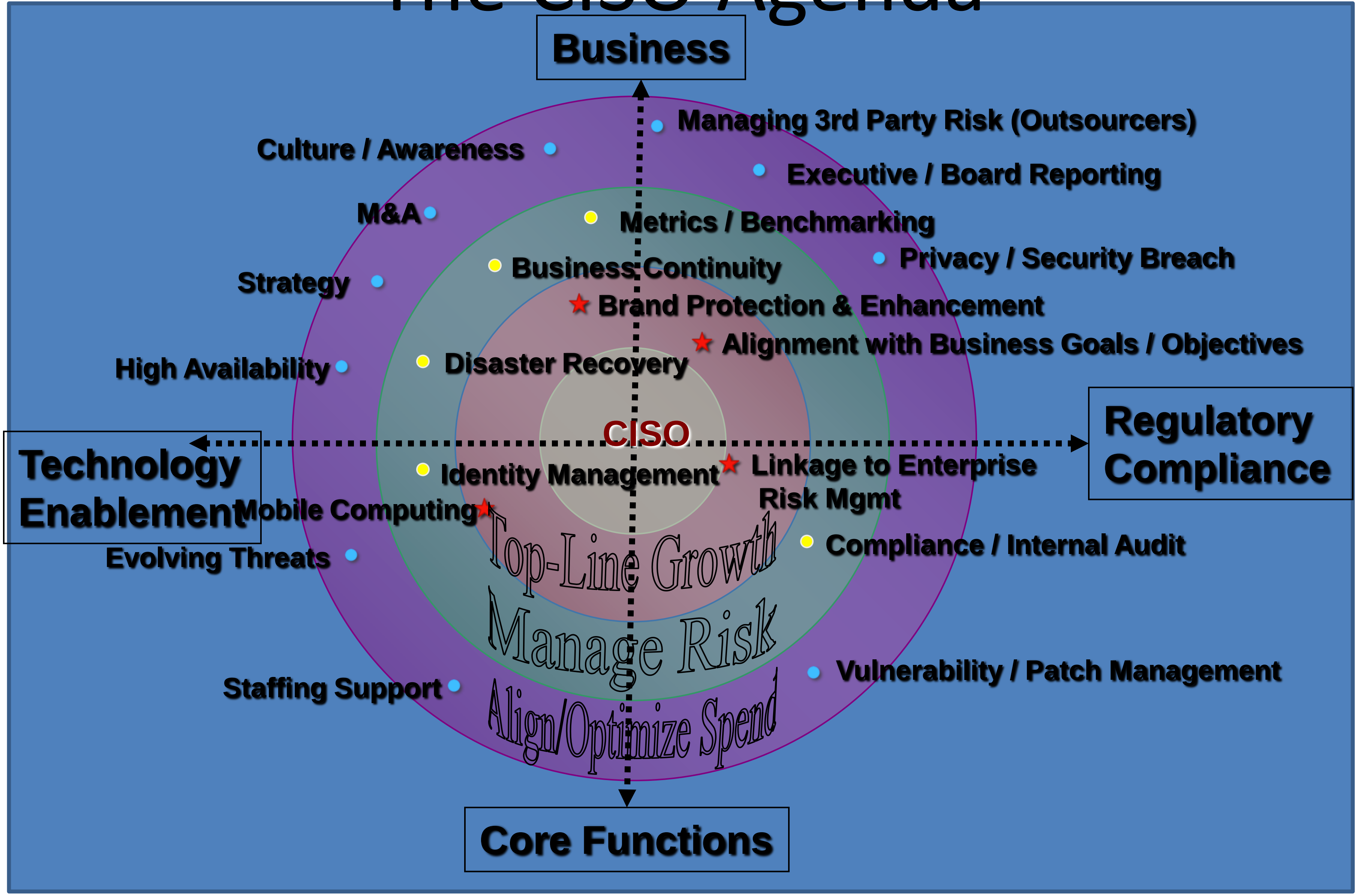
Northwestern University
Network Security

Topics for Discussion
What do you want to talk about?

- IT Security in the Business
- Policies, Standards, and Procedures
- Security Reality and Automation
- Measurement and Metrics in Security

The CISO Agenda



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:

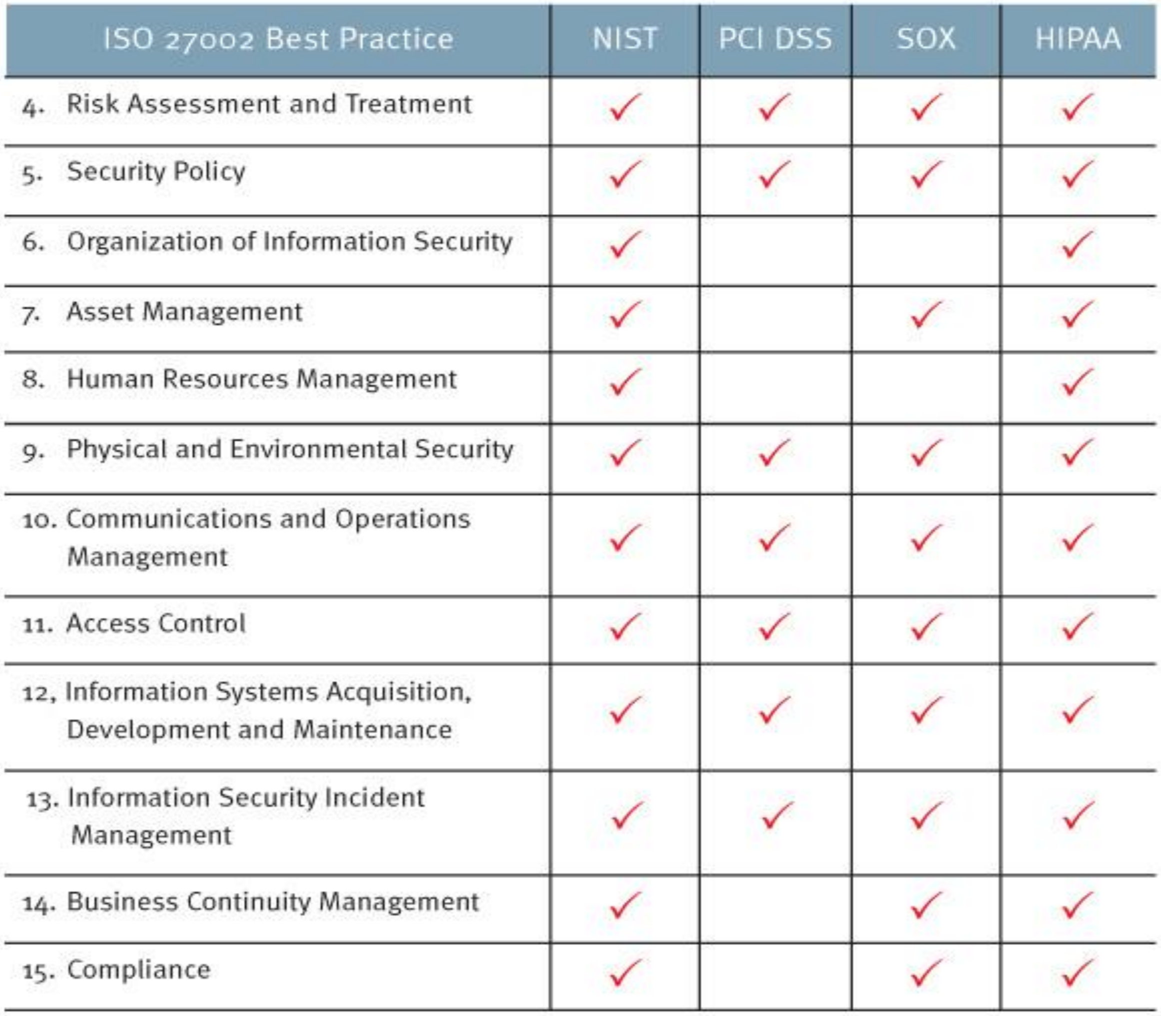
- Policies and Standards
- Security and Configuration baselines
- Framework use – ISO, COBIT, ITIL, GAISP, NIST
- Best Practices

Compliance cont’d

External compliance:

- SOX (Sarbanes Oxley)
  - COSO Framework
- HIPAA
- PCI
- Safe Harbor

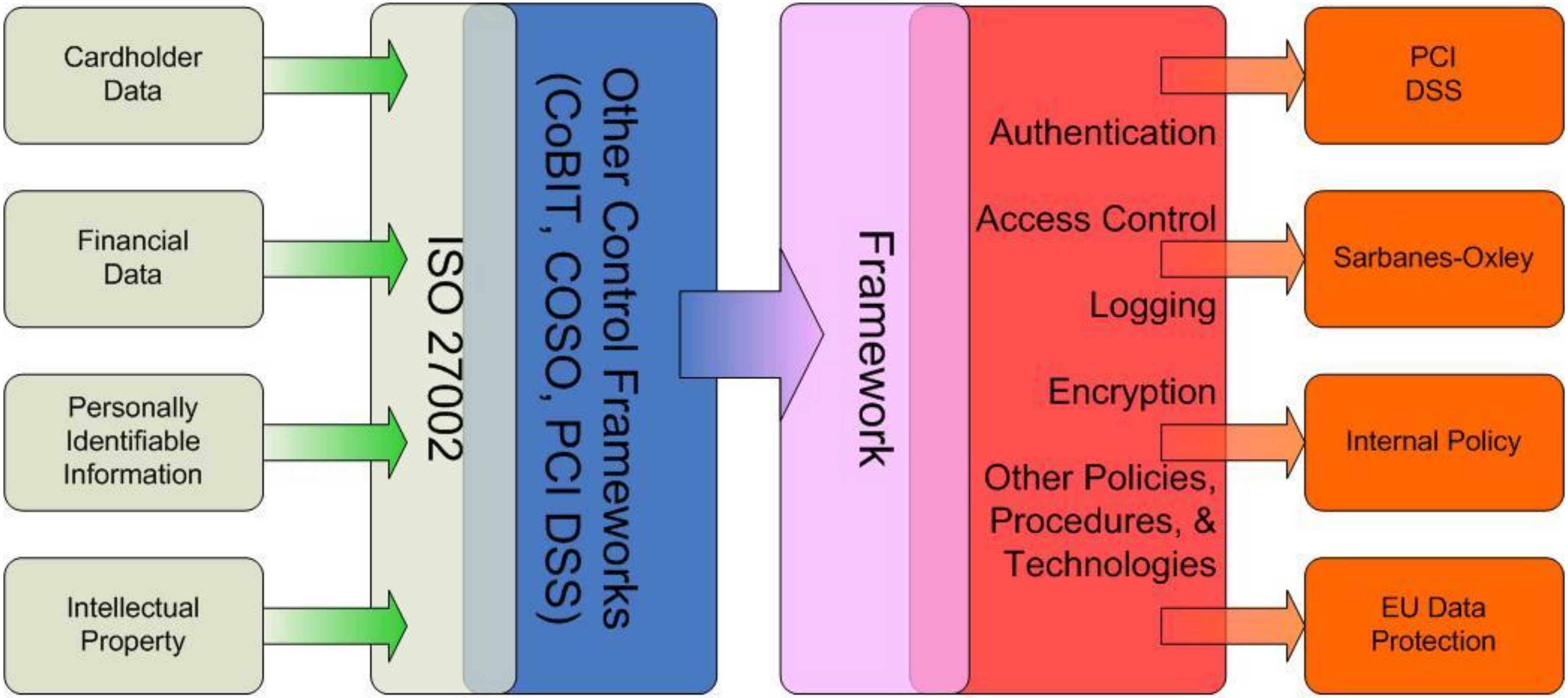
ISO Leading Practices



ISO 27002 Best Practice	NIST	PCI DSS	SOX	HIPAA
4. Risk Assessment and Treatment	✓	✓	✓	✓
5. Security Policy	✓	✓	✓	✓
6. Organization of Information Security	✓			✓
7. Asset Management	✓		✓	✓
8. Human Resources Management	✓			✓
9. Physical and Environmental Security	✓	✓	✓	✓
10. Communications and Operations Management	✓	✓	✓	✓
11. Access Control	✓	✓	✓	✓
12, Information Systems Acquisition, Development and Maintenance	✓	✓	✓	✓
13. Information Security Incident Management	✓	✓	✓	✓
14. Business Continuity Management	✓		✓	✓
15. Compliance	✓		✓	✓

Source: www.rsa.com

Compliance in Action



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:

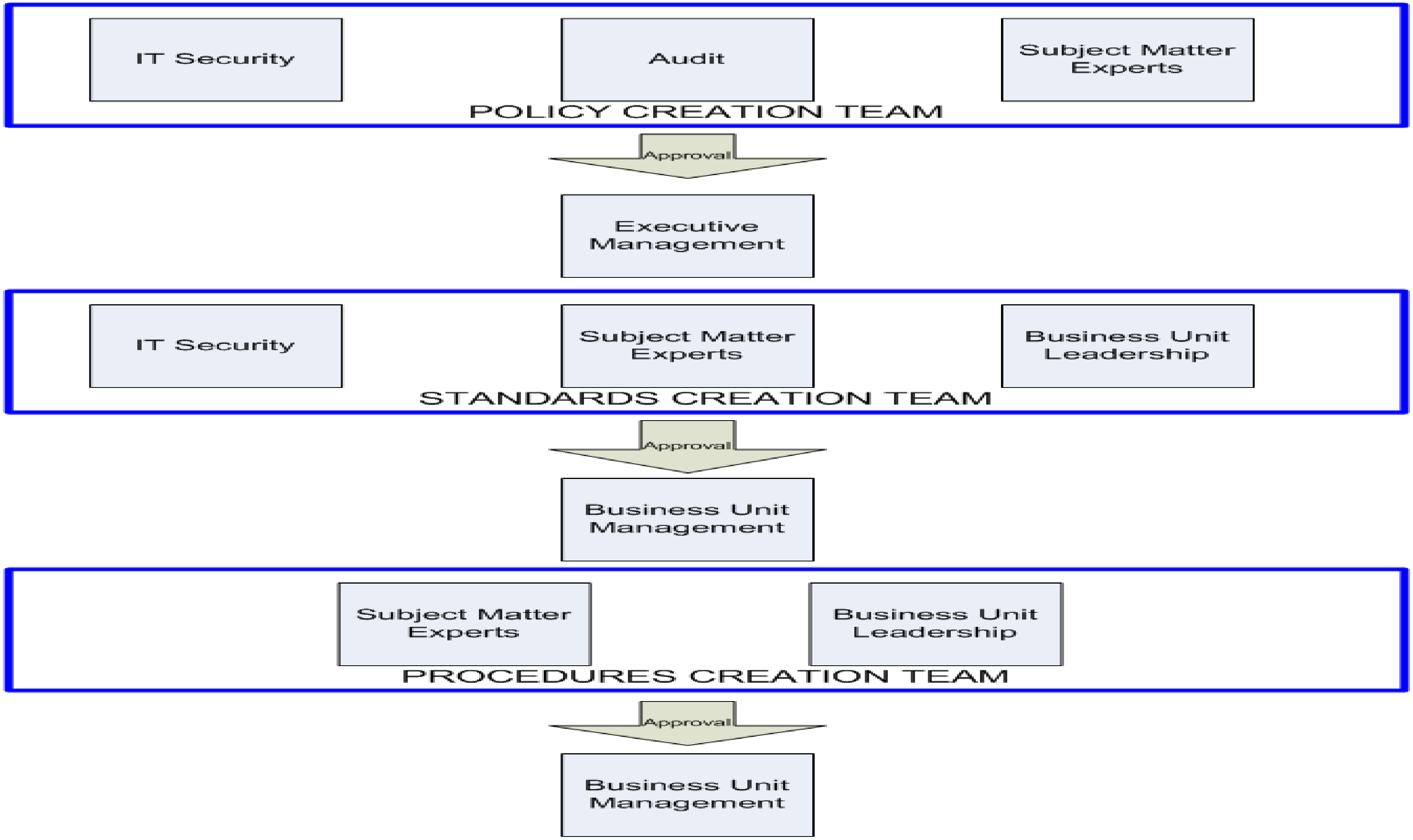
- Understanding of audit roles and procedures
- Familiarity with all systems, networks, and applications
- Compliance considerations

Internal Policy cont’d

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



IT Security

Audit

Subject Matter Experts

POLICY CREATION TEAM

Approval

Executive Management

IT Security

Subject Matter Experts

Business Unit Leadership

STANDARDS CREATION TEAM

Approval

Business Unit Management

Subject Matter Experts

Business Unit Leadership

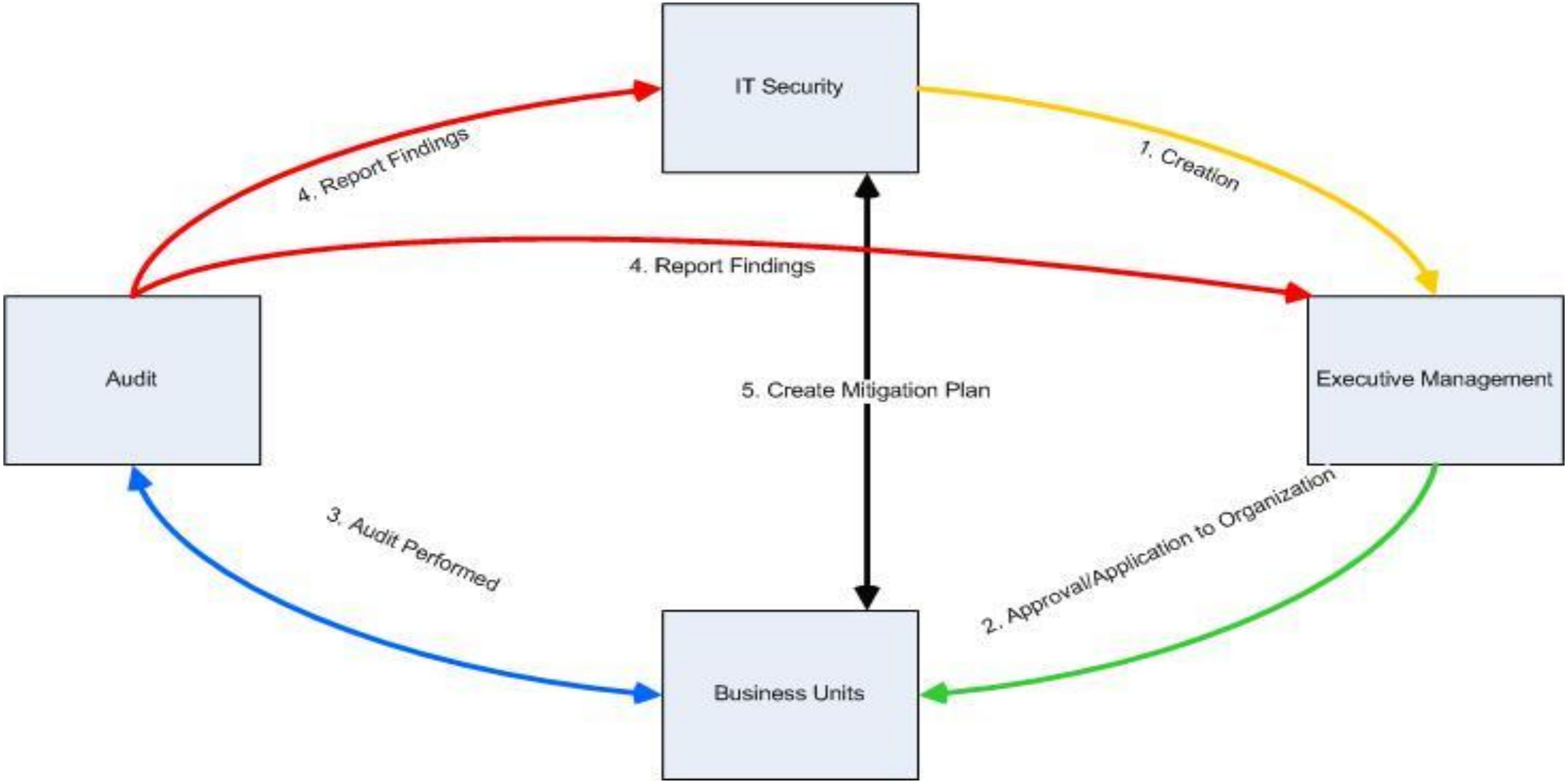
PROCEDURES CREATION TEAM

Approval

Business Unit Management

Internal Policy cont'd

Policy creation and enforcement cycle



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…

Policy Business Case cont’d

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

Cryptography and
ey Management Polic

Network
Configuration Policy

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

Attacks are increasingly publicized

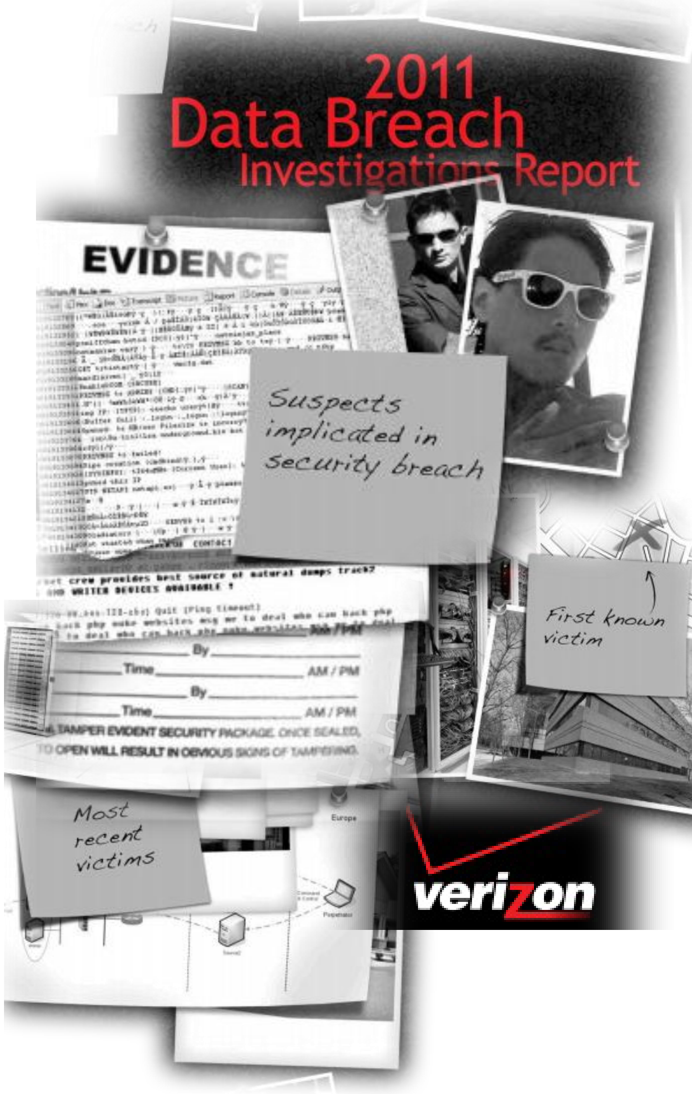
Advanced Persistent Threat (Aurora, RSA)

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?

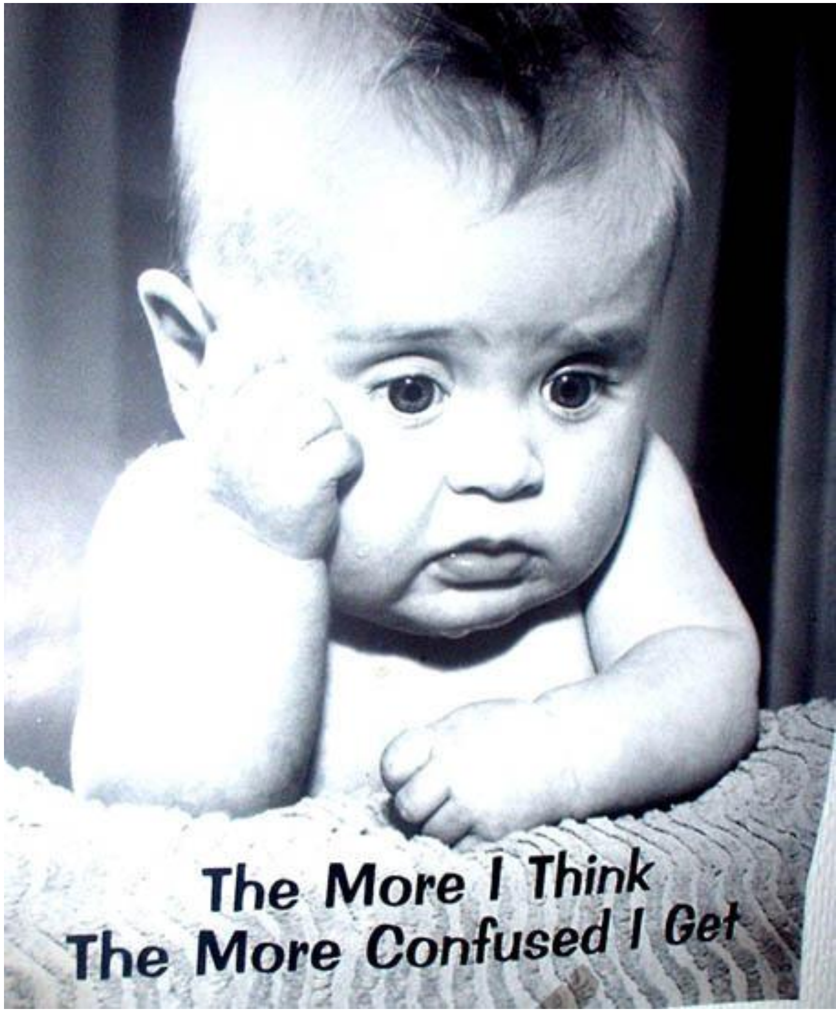

2011
Data Breach
Investigations Report
EVIDENCE
Suspects implicated in security breach
First known victim
Most recent victims
TAMPER EVIDENT SECURITY PACKAGE. ONCE SEALED, TO OPEN WILL RESULT IN OBVIOUS SIGNS OF TAMPERING.
verizon

The paradox

Let’s review:

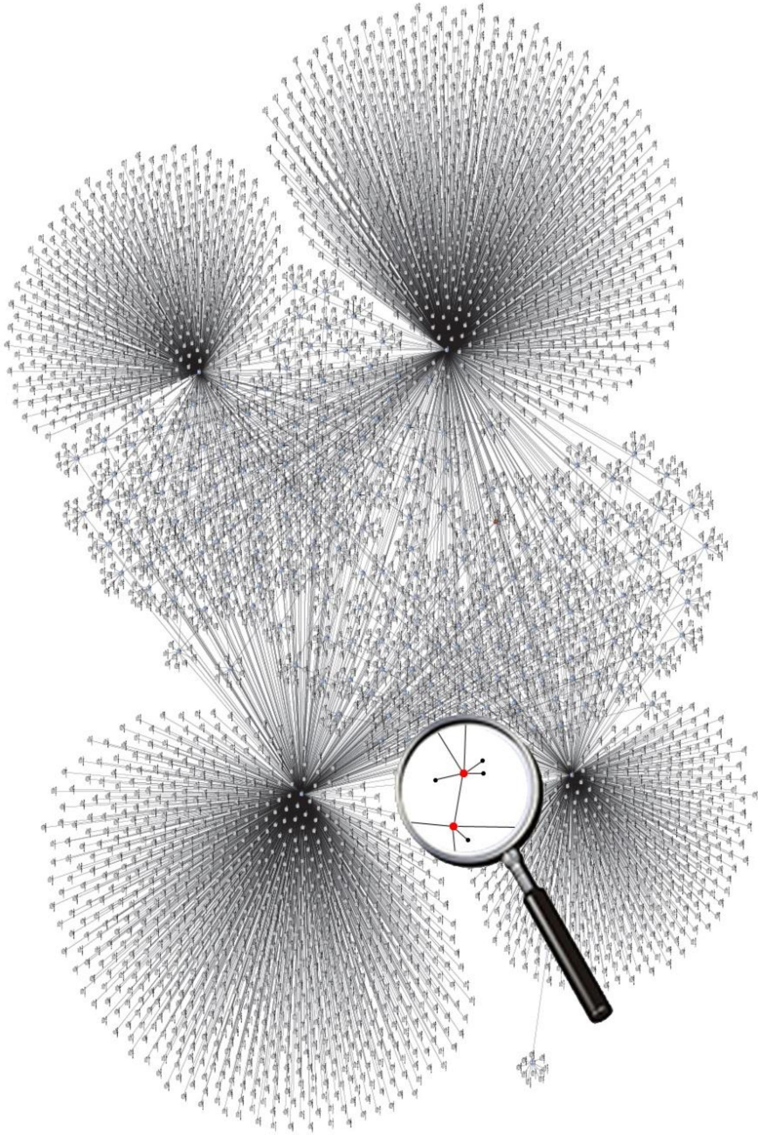
1. Bad guys are getting in
2. We’re spending billions
3. Simple controls work

What’s going wrong?

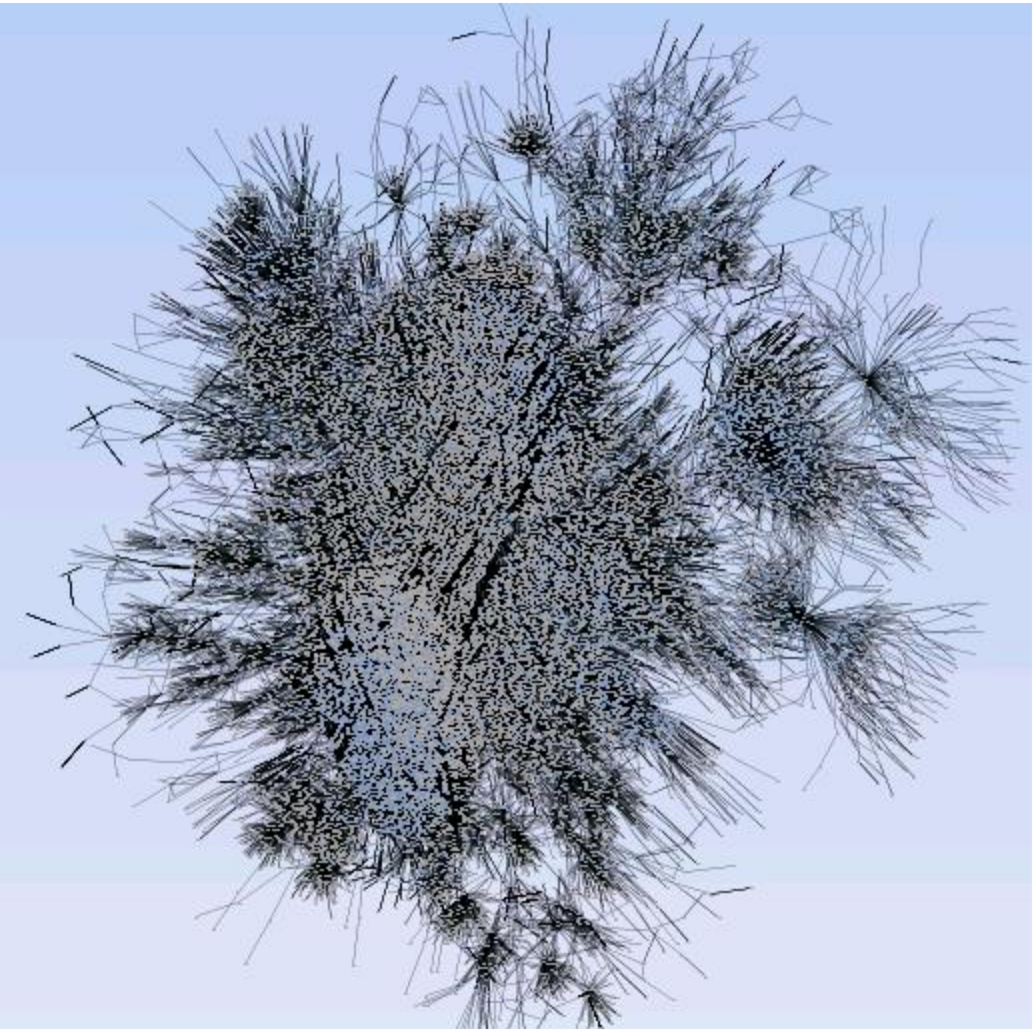


Complexity is the enemy

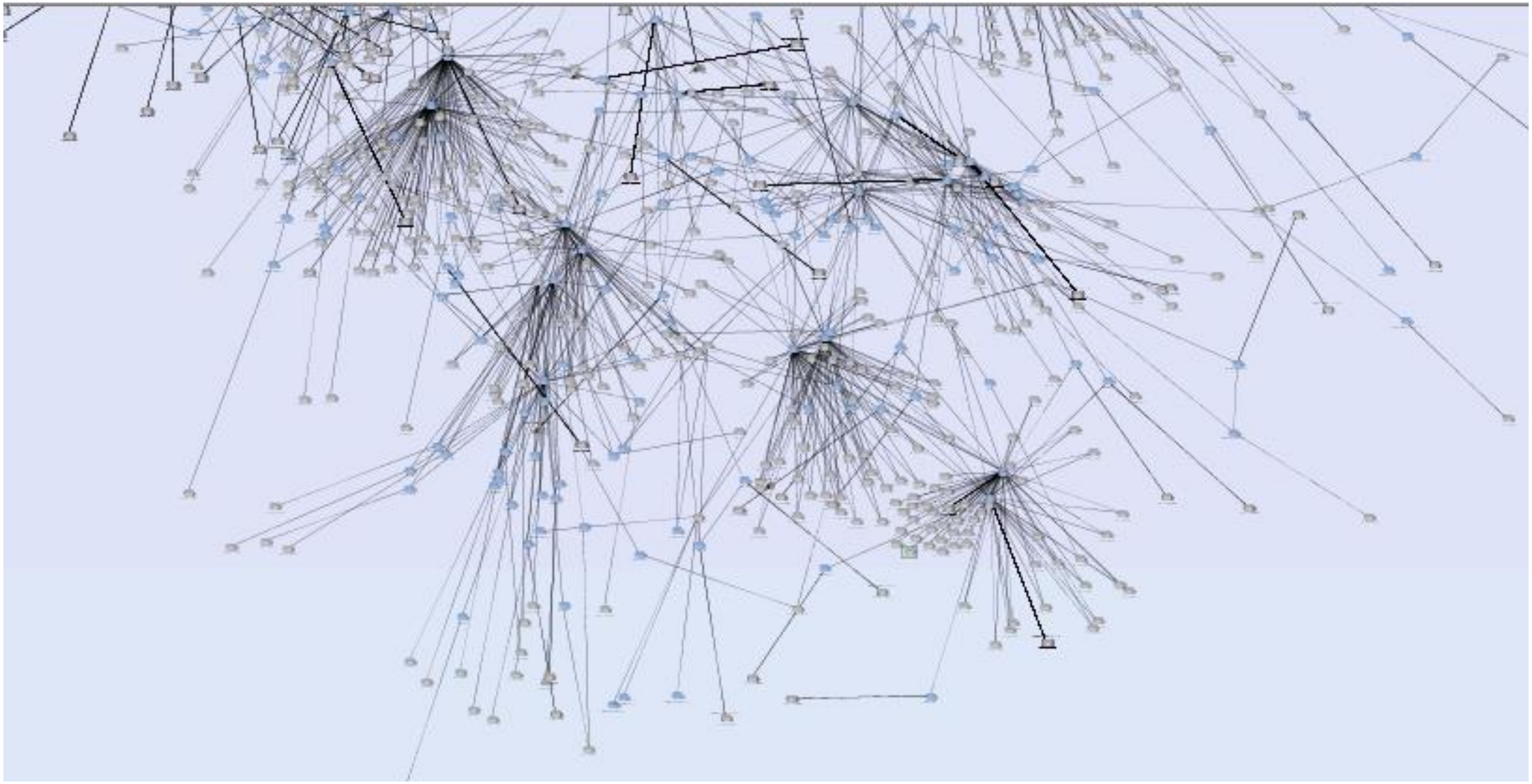
- Verizon said “consistent” controls
  - In real networks, that’s hard
  - Complexity defeats us
- Humans don’t handle complexity well
- We set policy well
- Human effort just doesn’t scale
  - Too many details
  - Too many interactions
- Just how complex are real world infrastructures?



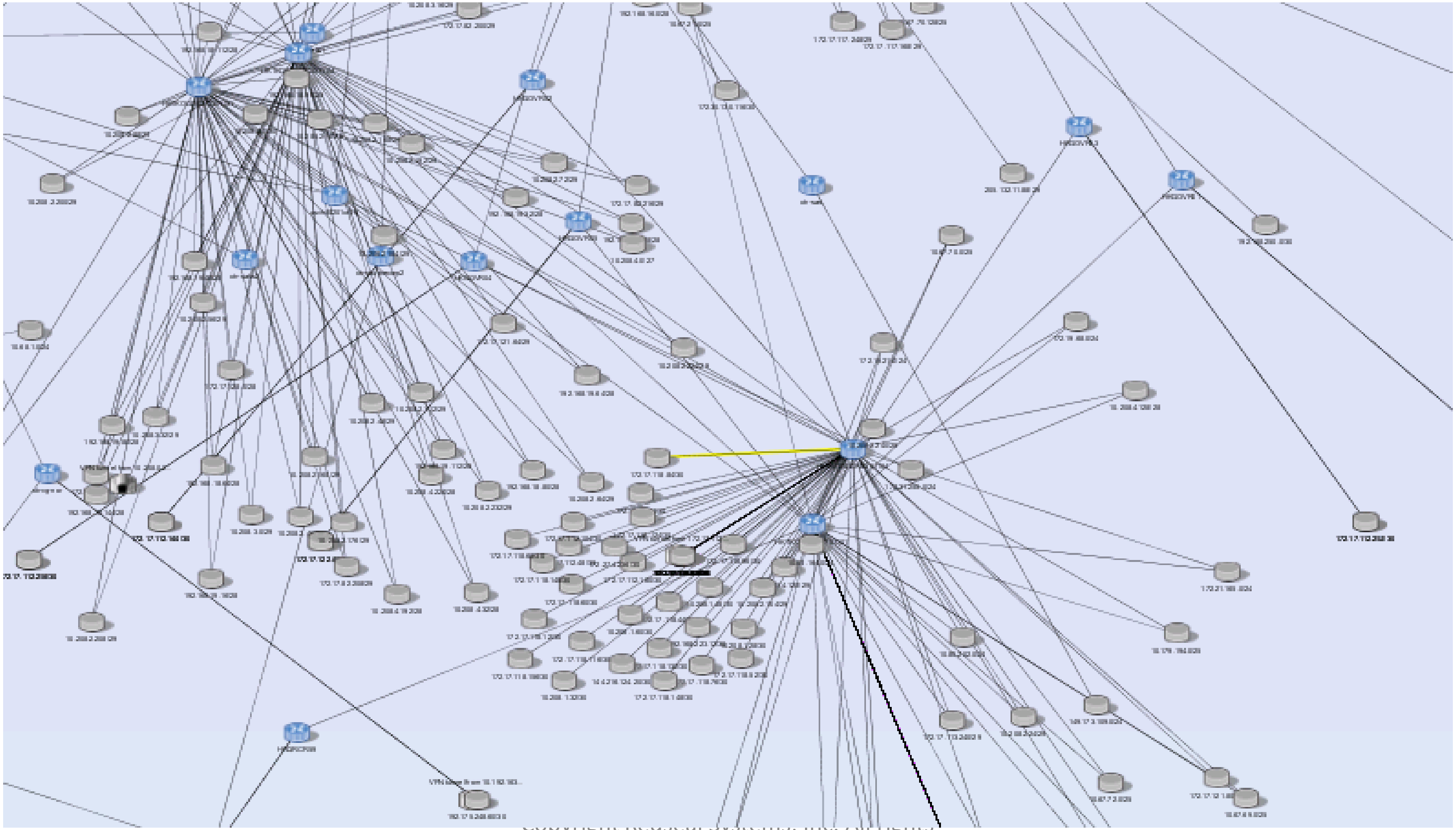
Here’s one real corporate network



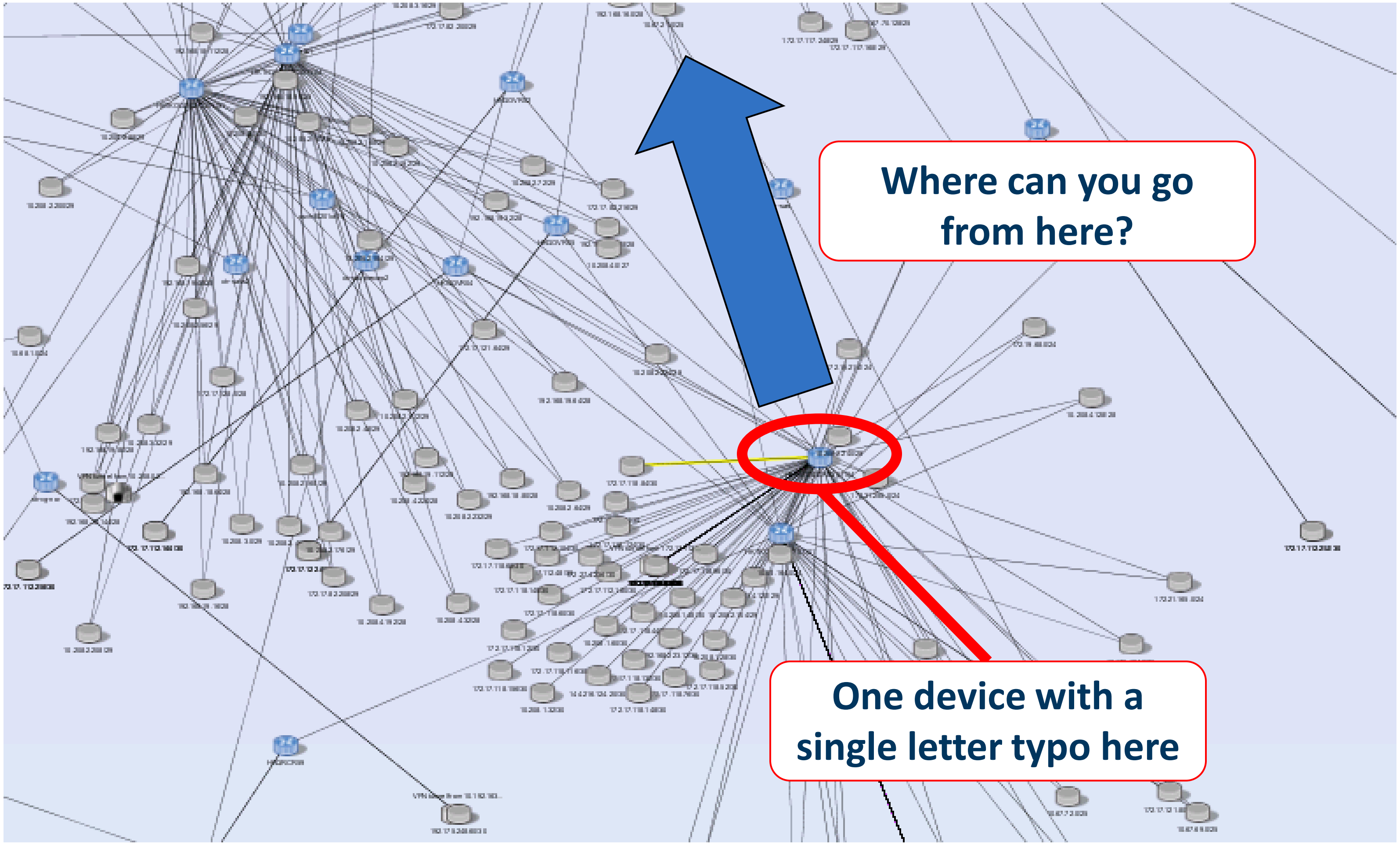
Zooming in a bit…



Here’s one “doorway” into the network



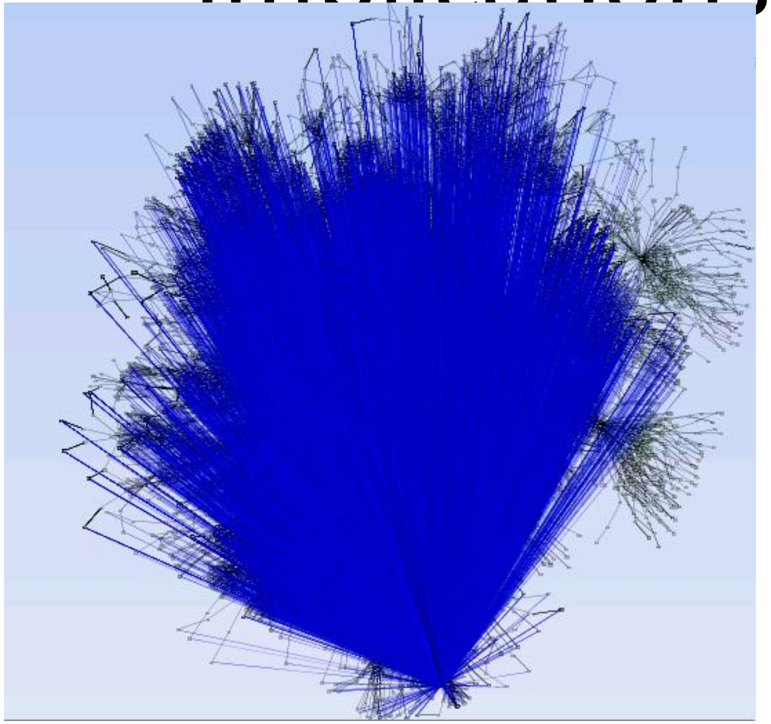
One small typo created a problem



Where can you go from here?

One device with a single letter typo here

Implications of simple typo



Technical details:

- ACL as written:

```
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:

```
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

Steve Honda/AFP/Getty Images

Garry Kasparov during his rematch against the IBM supercomputer Deep Blue, 1997

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

Security Metrics

- Security is the **absence** of something
- Can't report how often you were **NOT** on the cover of WSJ

Measuring Busy-ness

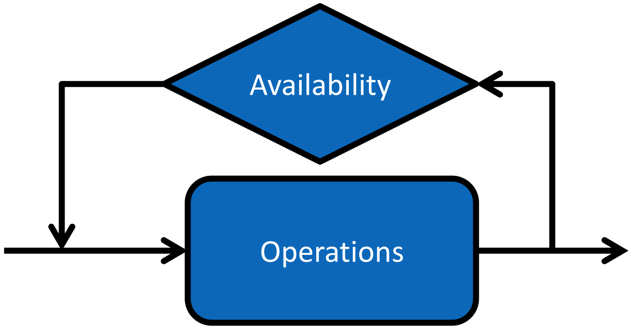
- Many people start with process counting

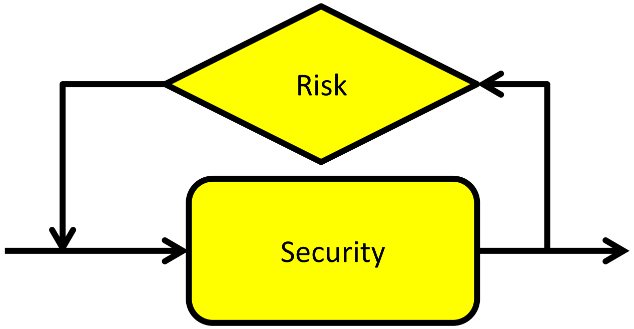
- These measure **busyness**
  - Not business

- How do you show gains?
  - Just get busier?

Management Metrics

- Metrics close the control loop
- Ops has availability
- Security needs risk
- Focus on outcomes
  - How easily could a breach occur?
  - How effective is our spend?
  - Are we making it harder to break in?





Resources Required

- Assets you need to protect
  - Everyone has some examples
    - PII, regulatory assets, IP, etc
  - Some truly “mission critical”
    - Financial, energy, government, military

- Knowledge of vulnerabilities
  - Bad guys exploit them, so you scan

- Counter-measures
  - It starts with the firewall

Be PROACTIVE

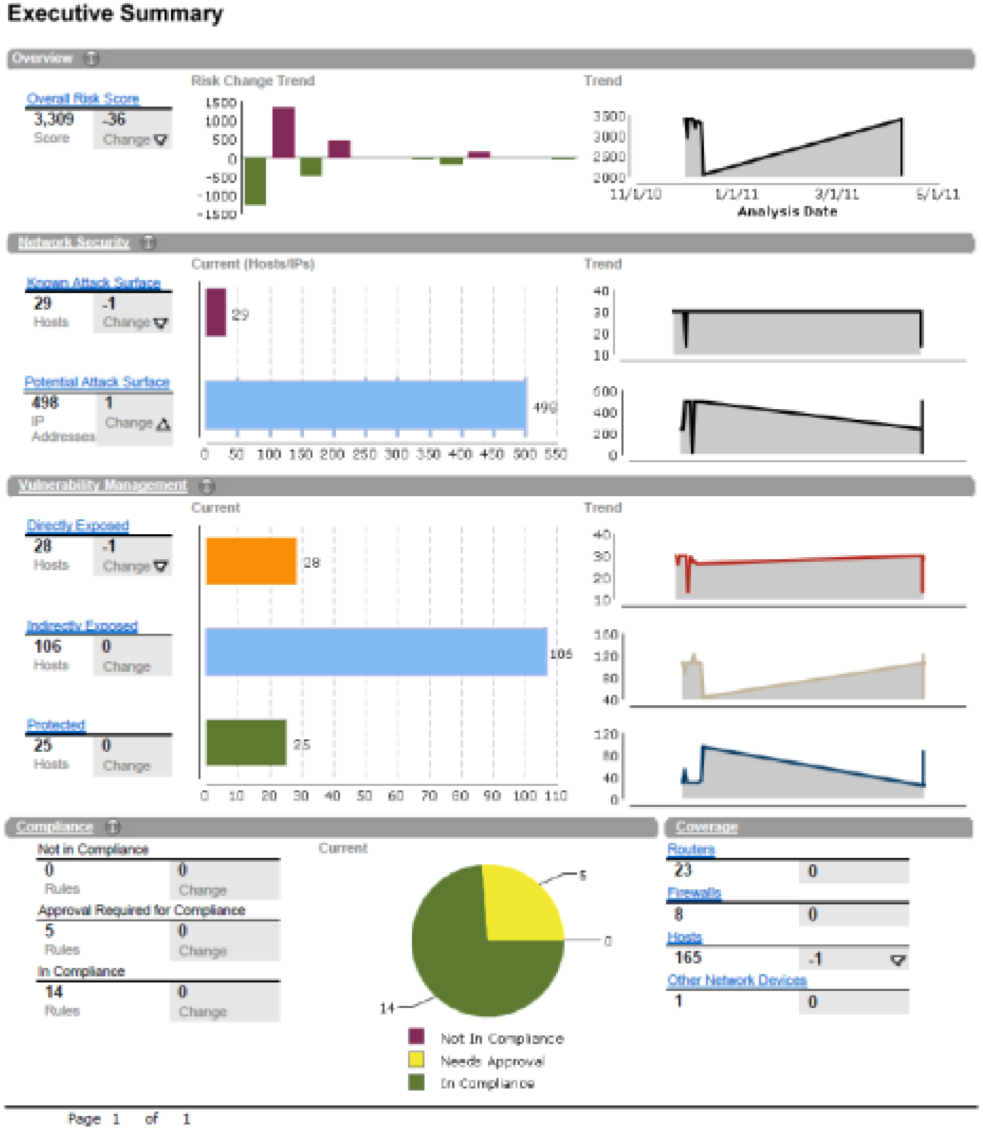
- We want to know our defensive posture
- That involves finding the weak points
- Attack a model of the network
- Measure ease of compromise
  - Use standards where possible

Outbound Proof

How easily can attackers get in?

How big is my attack surface?

How much is non-compliant?



Executive Summary

Overview

Overall Risk Score
3,309 Score
-36 Change ▽

Network Security

Known Attack Surface
29 Hosts
-1 Change ▽

Potential Attack Surface
498 IP Addresses
1 Change △

Vulnerability Management

Directly Exposed
28 Hosts
-1 Change ▽

Indirectly Exposed
106 Hosts
0 Change

Protected
25 Hosts
0 Change

Compliance

Not in Compliance
0 Rules
0 Change

Approval Required for Compliance
5 Rules
0 Change

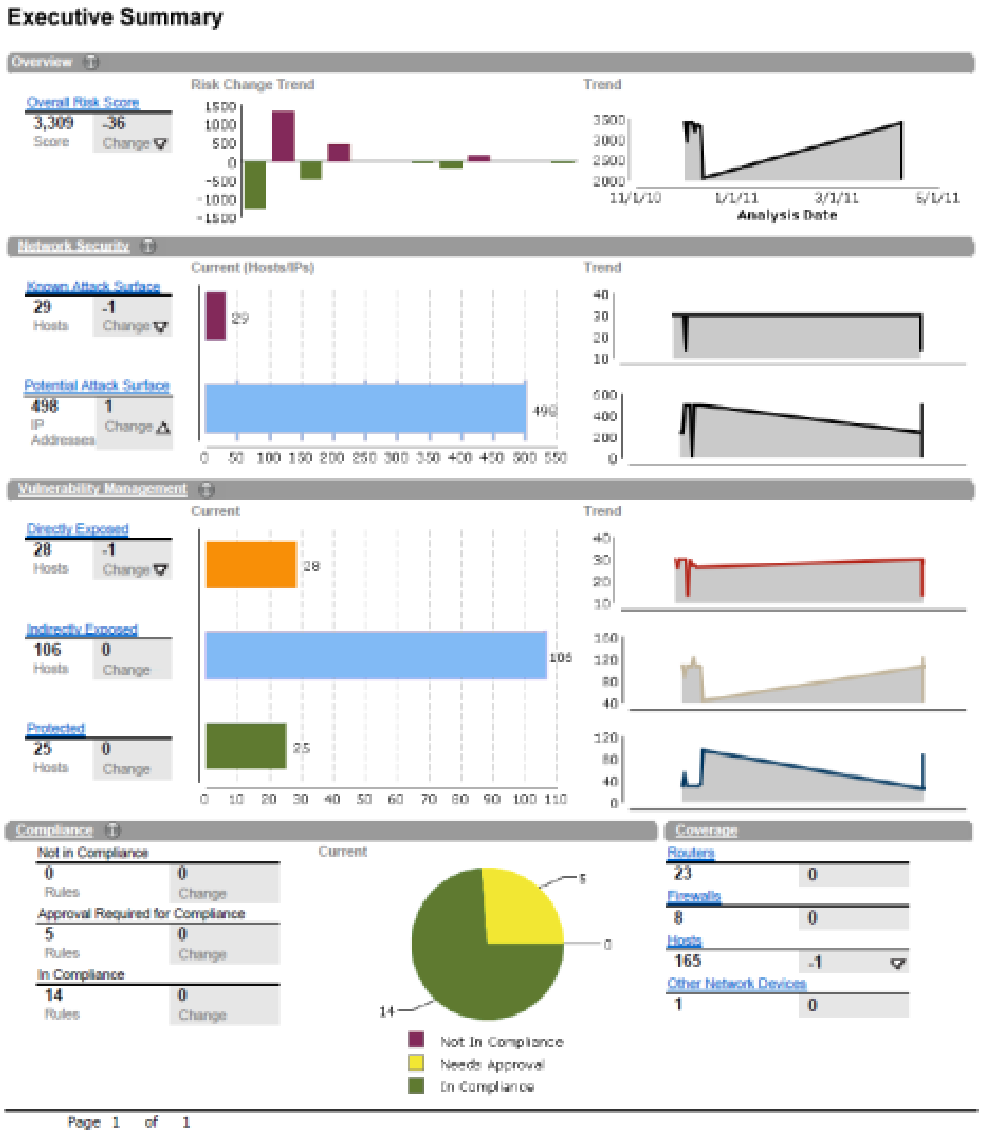
In Compliance
14 Rules
0 Change

Coverage

Routers	
23	0
Firewalls	
8	0
Hosts	
165	-1 ▽
Other Network Devices	
1	0

Page 1 of 1

Dashboards for Internal



Executive Summary

Overview

Overall Risk Score

3,309 Score

-36 Change

Network Security

Known Attack Surface

29 Hosts

-1 Change

Potential Attack Surface

498 IP Addresses

1 Change

Vulnerability Management

Directly Exposed

28 Hosts

-1 Change

Indirectly Exposed

106 Hosts

0 Change

Protected

25 Hosts

0 Change

Compliance

Not in Compliance

0 Rules

0 Change

Approval Required for Compliance

5 Rules

0 Change

In Compliance

14 Rules

0 Change

Coverage

Routers

23 0

Firewalls

8 0

Hosts

165 -1

Other Network Devices

1 0

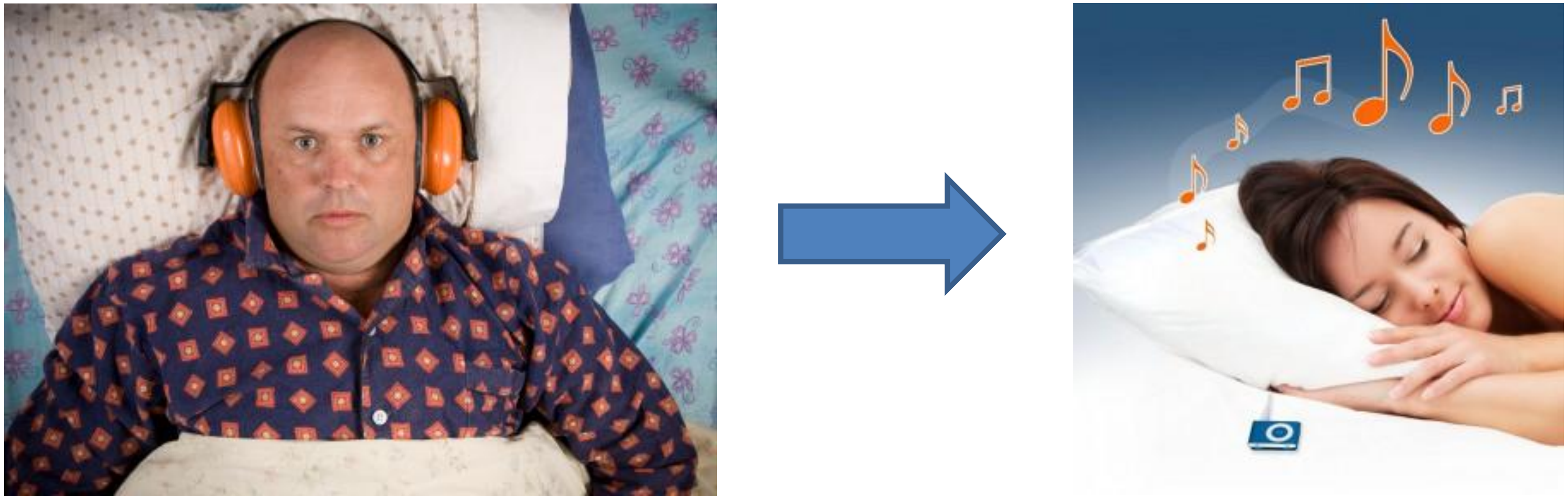
Page 1 of 1

Are investments working?

Where do we need to improve?

Metrics Conclusions

- Defensive posture **CAN** be measured
- This drives to better outcomes
  - Measure posture => improved posture
- It helps the CFO “get it”
- You can sleep better
  - Demonstrate effectiveness, not busyness



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
- Without effective metrics, security will never get the exposure or support needed from the top down

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

Security Practitioners

Let’s look at some poll results of the real world of security:

Survey Graphic

Options

Defensive Options:

This is not a pitch so ask offline if you want ideas on what’s out there and effective ☺

Offensive:

<< back|track-linux.org

Backtrack

- Backtrack is a Linux based hacking toolkit provided by the people at 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

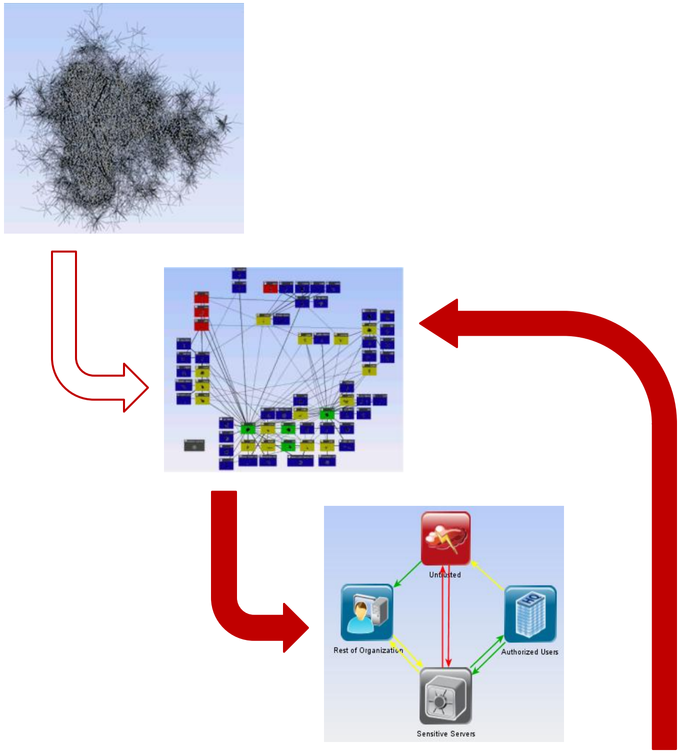
Backtrack

- 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

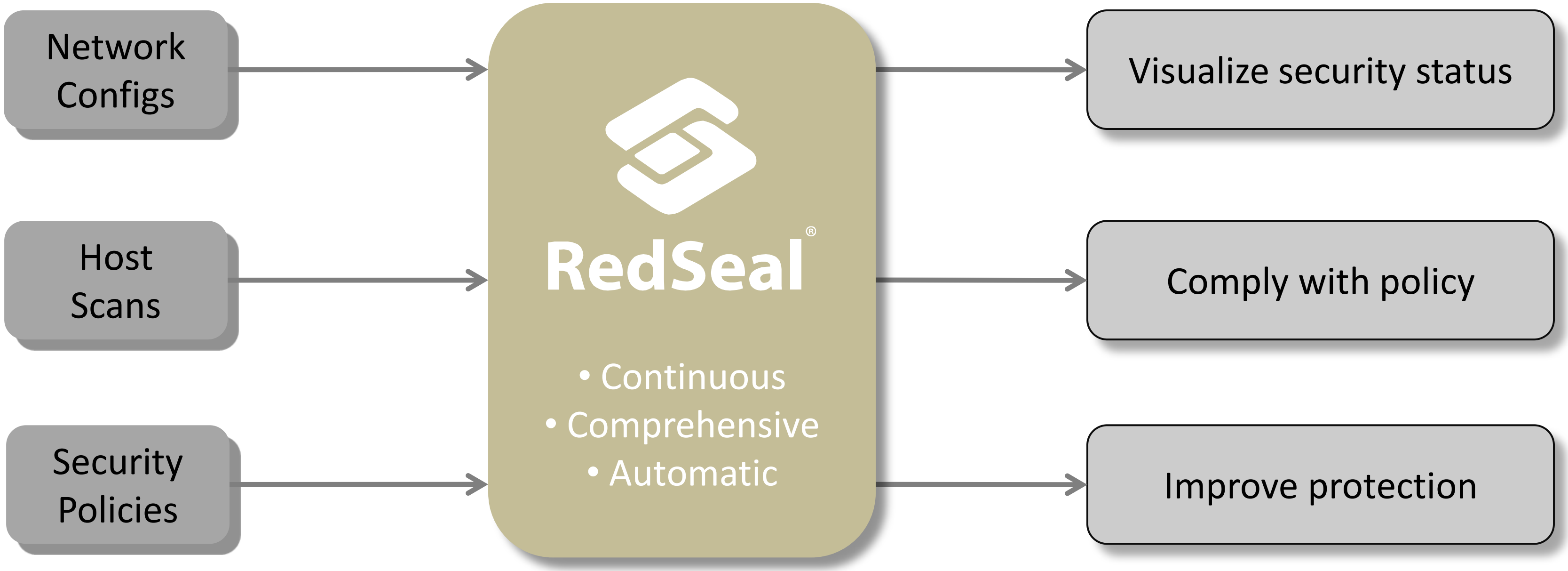


- Visualize
  - End to end infrastructure
- Comply
  - Test network controls
- Protect
  - Actionable remediation

Destination Host Start:211 End:271 Change:+60 Percent Change:+28%
Jul 06, 2011 17:24:52 - Jul 06, 2011 17:47:10
250
200
150
17:25
17:30
17:35
17:40
17:45
Jul 11
Jul 18
Jul 25
Custom period: 2011-07-06 17:24:52 - 2011-07-06 17:47:10
Zoom: 10D YTD MAX

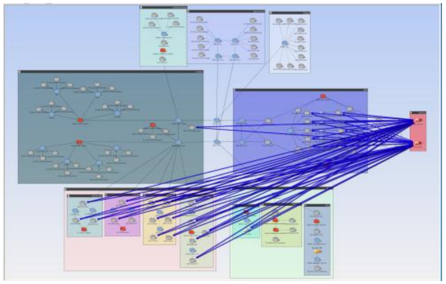
Automated & continuous

Three key questions

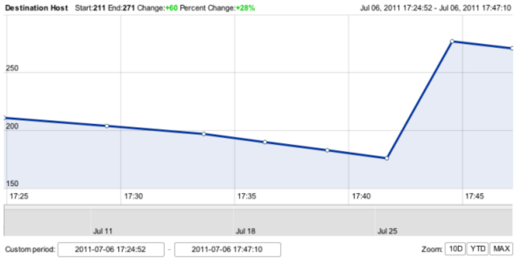


- Technology to answer:
  1. Where are your high risk vulnerabilities?
  2. Am I compliant with network security policy?
  3. How are IT changes impacting my security over time?

Visualize your network security



Immediately understand security posture

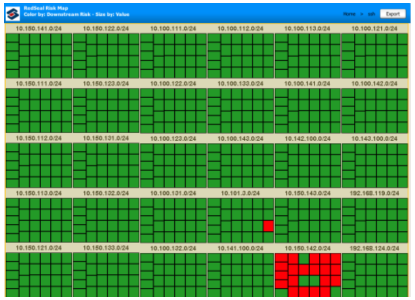


Destination Host Start:**211** End:**271** Change:+60 Percent Change:+28%

Jul 06, 2011 17:24:52 - Jul 06, 2011 17:47:10

Custom period: 2011-07-06 17:24:52 - 2011-07-06 17:47:10

Communicate return on security investments

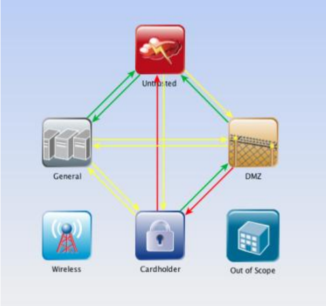


RedSeal Risk Map
Color by: Downstream Risk - Size by: Value

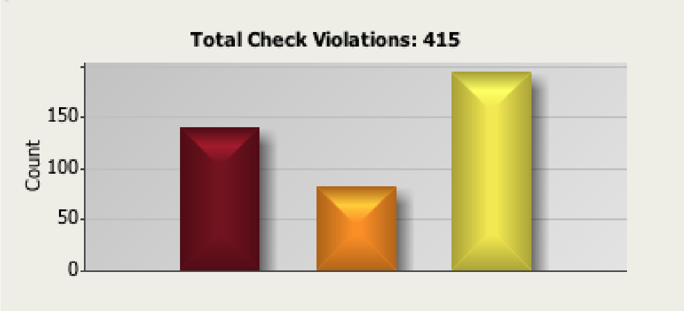
10.150.141.0/24	10.150.122.0/24	10.100.111.0/24	10.100.112.0/24	10.100.113.0/24	10.100.121.0/24
10.150.111.0/24	10.150.123.0/24	10.100.122.0/24	10.100.133.0/24	10.100.141.0/24	10.100.142.0/24
10.150.112.0/24	10.150.131.0/24	10.100.123.0/24	10.100.143.0/24	10.142.100.0/24	10.143.100.0/24
10.150.113.0/24	10.150.132.0/24	10.100.131.0/24	10.101.3.0/24	10.150.143.0/24	192.168.119.0/24
10.150.121.0/24	10.150.133.0/24	10.100.132.0/24	10.141.100.0/24	10.150.142.0/24	192.168.124.0/24

Detect anomalies & patterns

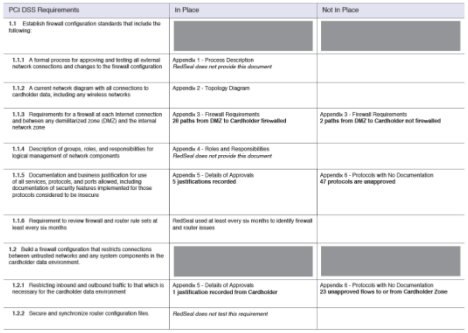
Continuously **comply** with policy



Continuously monitor network for compliance



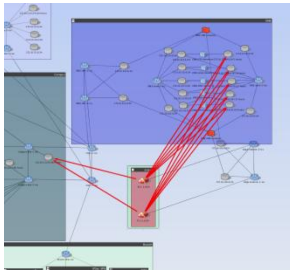
Enforce industry recommended & custom configuration best practices



PCI DSS Requirements	In Place	Not In Place
1.1 Establish firewall configuration standards that include the following:		
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	Appendix 1 - Process Description *RedSeal does not provide this document*	
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	Appendix 2 - Topology Diagram	
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Appendix 3 - Firewall Requirements **28 paths from DMZ to Cardholder firewalled**	Appendix 3 - Firewall Requirements **2 paths from DMZ to Cardholder not firewalled**
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	Appendix 4 - Roles and Responsibilities *RedSeal does not provide this document*	
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	Appendix 5 - Details of Approvals **5 justifications recorded**	Appendix 6 - Protocols with No Documentation **47 protocols are unapproved**
1.1.6 Requirement to review firewall and router rule sets at least every six months	RedSeal used at least every six months to identify firewall and router issues	
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.		
1.2.1 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	Appendix 5 - Details of Approvals **1 justification recorded from Cardholder**	Appendix 6 - Protocols with No Documentation **23 unapproved flows to or from Cardholder Zone**
1.2.2 Secure and synchronize router configuration files.	*RedSeal does not test this requirement*	

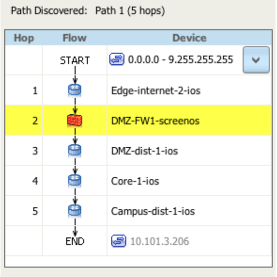
Demonstrate compliance to auditors

Protect yourself from compromise



Highlight gaps in security

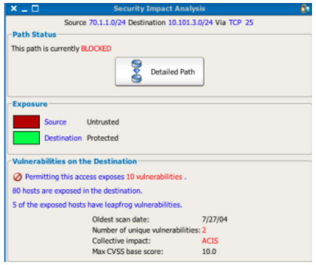
Identify high-risk vulnerabilities



Path Discovered: Path 1 (5 hops)

Hop	Flow	Device
	START	0.0.0.0 - 9.255.255.255
1		Edge-internet-2-ios
2		DMZ-FW1-screenos
3		DMZ-dist-1-ios
4		Core-1-ios
5		Campus-dist-1-ios
	END	10.101.3.206

Pin-point rules violating network policy



Security Impact Analysis

Source 70.1.1.0/24 Destination 10.101.3.0/24 Via TCP 25

Path Status

This path is currently BLOCKED

Exposure

🟥 Source Untrusted

🟩 Destination Protected

Vulnerabilities on the Destination

Permitting this access exposes 10 vulnerabilities .

80 hosts are exposed in the destination.

5 of the exposed hosts have leapfrog vulnerabilities.

Oldest scan date:	7/27/04
Number of unique vulnerabilities:	2
Collective impact:	ACIS
Max CVSS base score:	10.0

Assess risk of planned network changes