RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: DSP-W03

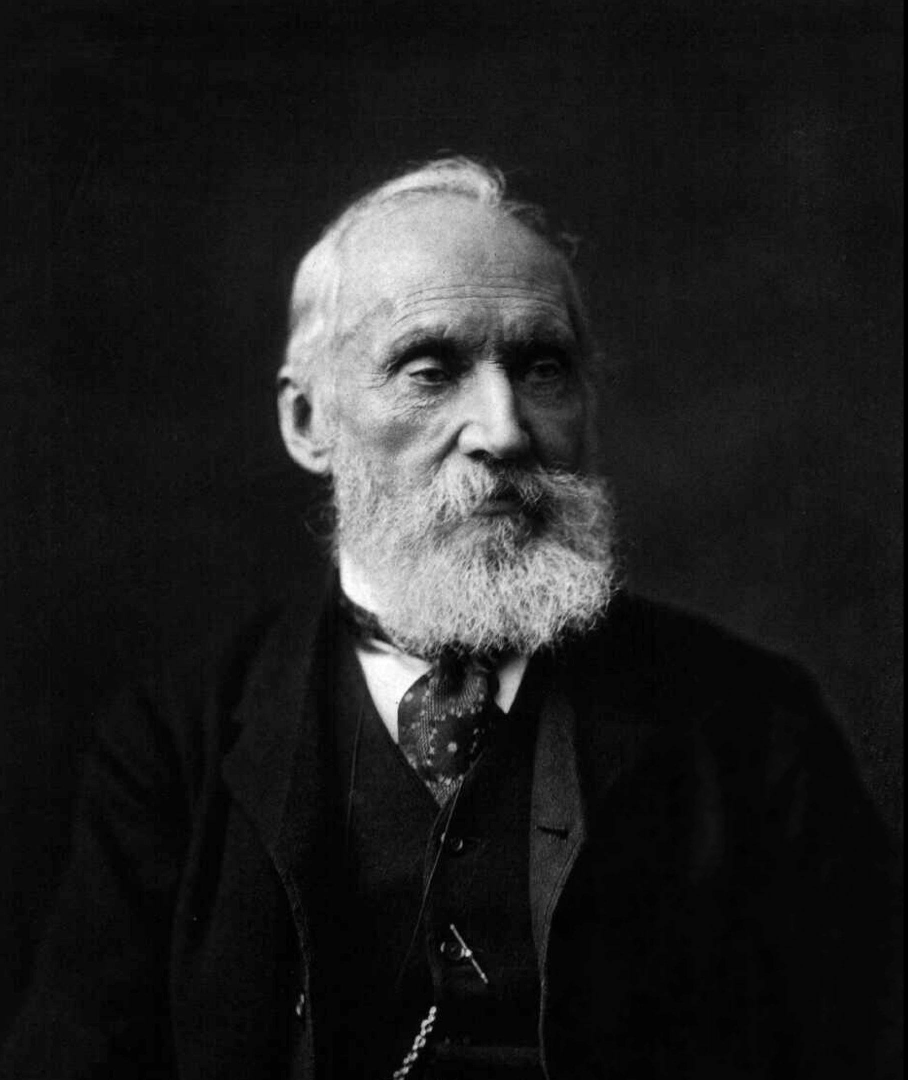
# The Kelvin Mantra: Implementing Data-Driven Security Practices

**Stephen Boyer**

Chief Technology Officer & Cofounder
BitSight Technologies
@swboyer

**Bob Rudis**

Security Data Scientist
Verizon Security Research (DBIR)
@hrbrmstr

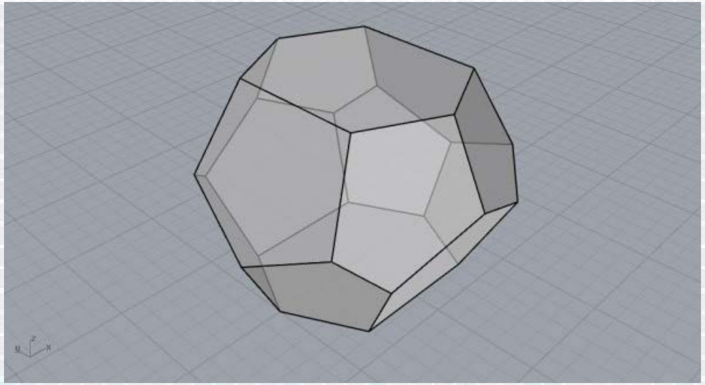


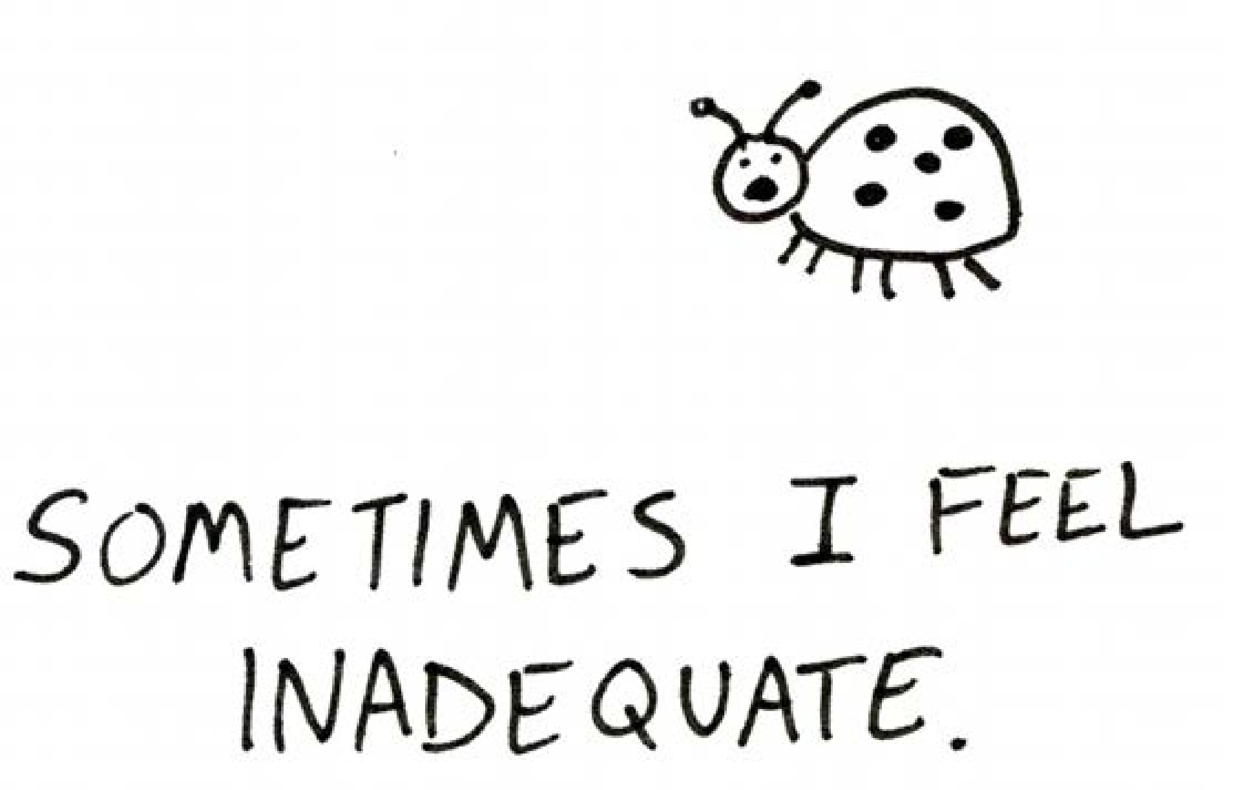
*If you can’t measure it, you can’t improve it*

290
310
330
270
350
DEGREES
KELVIN
WESTON

# William Thompson — Problem Solver

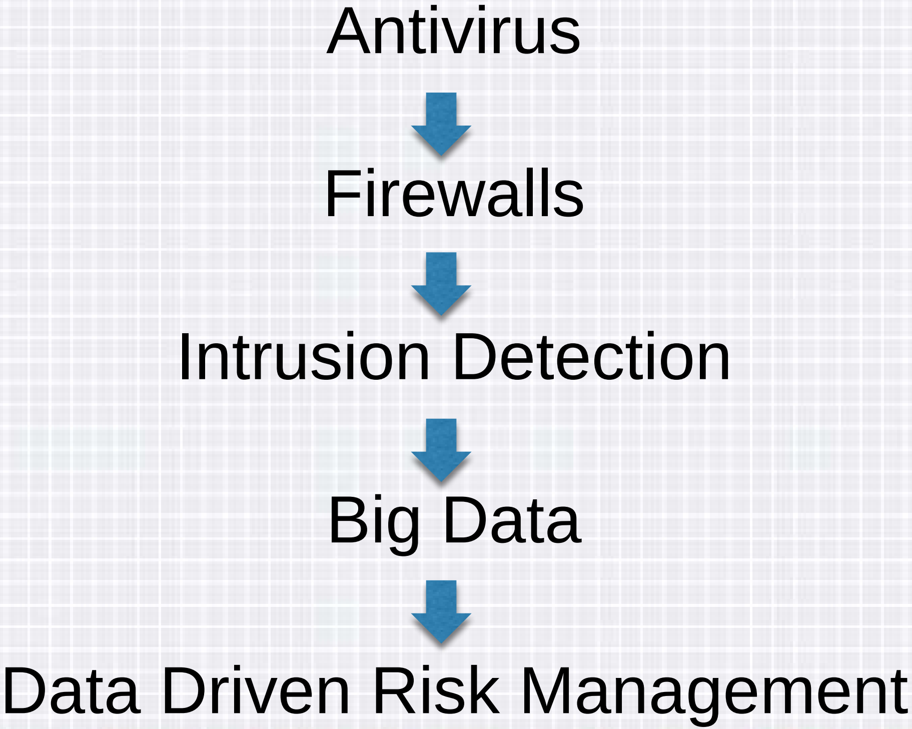
- The absolute temperature scale, now known as 'the Kelvin scale'
- The second law of thermodynamics
- Telegraph cables and the galvanometer
- Mariner’s compass; astronomical clock; echo (depth) sounders
- The tetrakaidecahedron.





SOMETIMES I FEEL INADEQUATE.

# Evolution of Cyber Security Approaches



Antivirus

Firewalls

Intrusion Detection

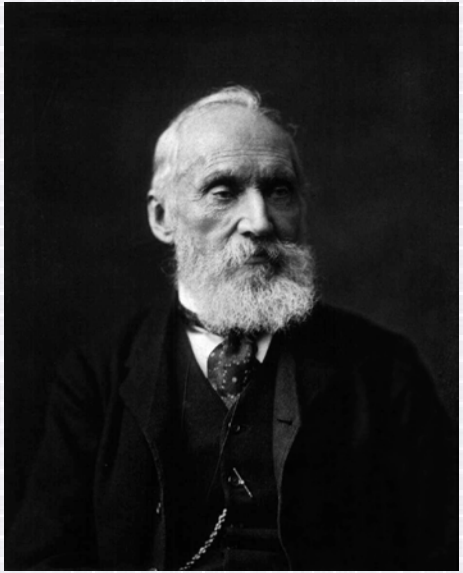
Big Data

Data Driven Risk Management

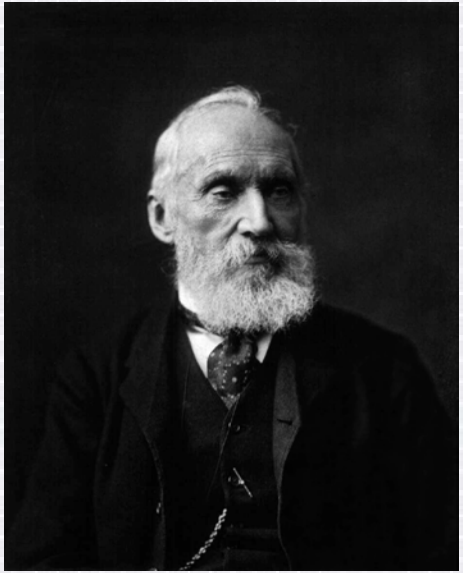
# Security → Risk Management

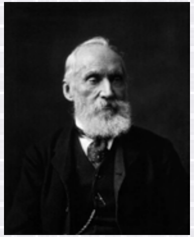
*What do **<u>you</u>** want to know?*

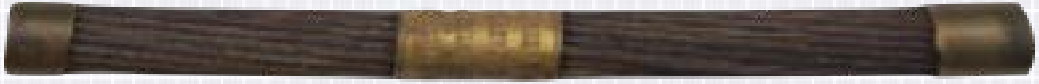
*What do you **think** you know?*



Dr Wildman Whitehouse





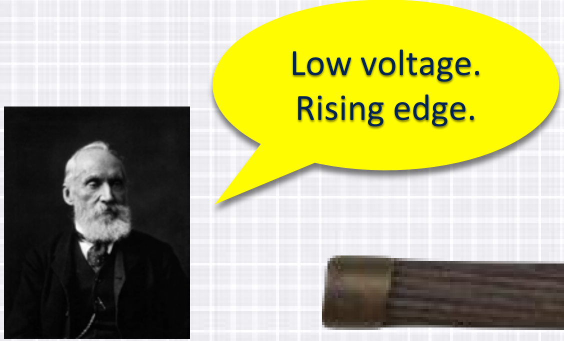


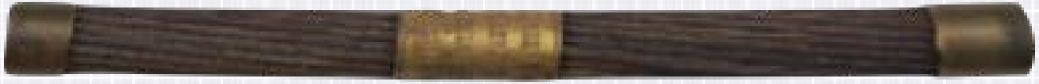
**“Engineer”**

- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •
Marketer/Promoter •
Tinkerer (Maker?)•



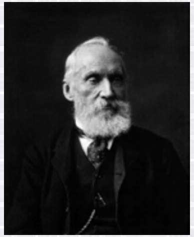


**“Engineer”**

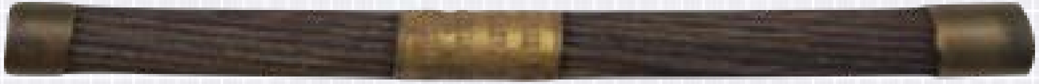
- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •
Marketer/Promoter •
Tinkerer (Maker?)•



Low voltage.
Rising edge.



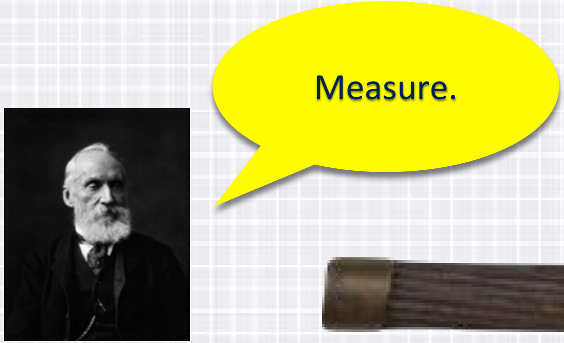
High voltage,
ba-by!

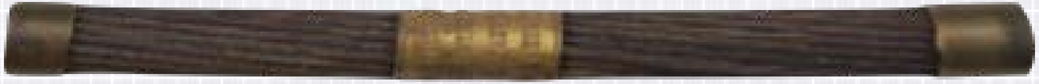
**“Engineer”**

- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •
Marketer/Promoter •
Tinkerer (Maker?)•



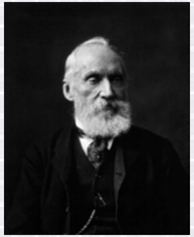


**“Engineer”**

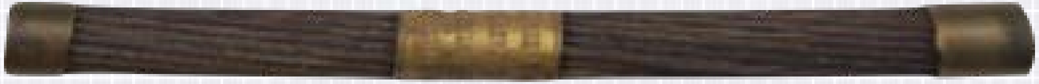
- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •
Marketer/Promoter •
Tinkerer (Maker?)•



Measure.



CRANK IT UP!

**“Engineer”**

- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •
Marketer/Promoter •
Tinkerer (Maker?)•

**“Engineer”**

- Scientist
- Researcher
- Deep Knowledge of Electricity

**“Thought Leader”**

(Good) Surgeon •

Marketer/Promoter •

Tinkerer (Maker?)•

# *What Should We Do To Reduce Risk?*

NAC!

IPS!

Advanced Malware Protection!

Threat Intelligence!

MOAR FIREWALLS!

# *What do you want to know?*

## Guiding Questions

# “Are *We* Secure?!”

- Board of Directors
- Senior Leadership
- General Council
- Internal Stakeholders

- Customers
- Patients
- Partners
- Investments / M&A

## “Are ***You*** Secure?!”

# Measurement Approaches:

- Inside Out
- Outside In

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

# *Inside Out:*

## Building A Data-Driven Security Risk Management Program

# So you want to measure risk…

- Understand who the **threat actors** are, and
- What **threat actions** they are likely to perform.
- Have a good handle on your **control strength,** and
- Know what controls are protecting **critical assets**.
- Have some idea of the **impact** of an incident or breach,
- as well as **incidents** you've already had.

Threat actors.

Threat actions.

# Threat Actors/Actions — TARA + VERIS

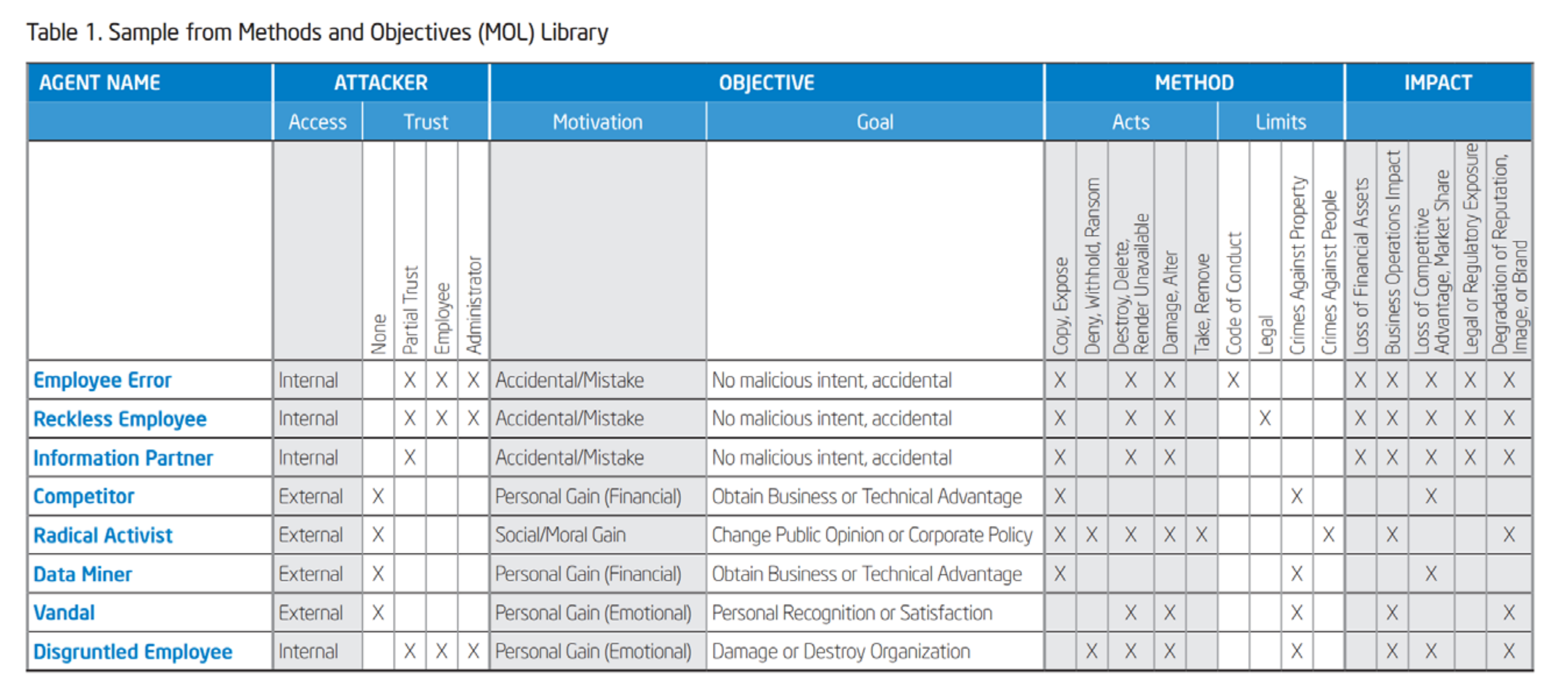
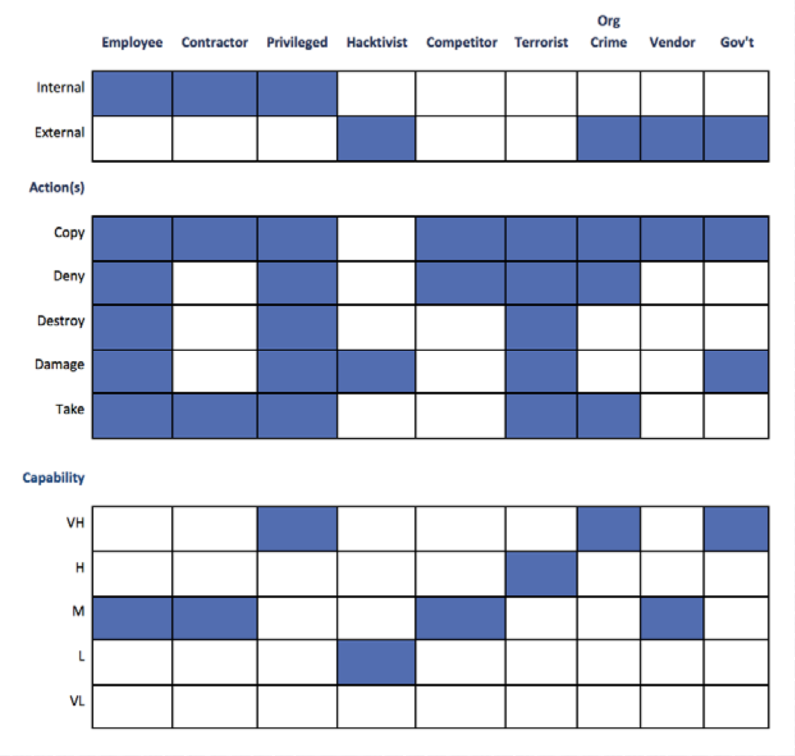


Table 1. Sample from Methods and Objectives (MOL) Library

| AGENT NAME | ATTACKER | | | | | OBJECTIVE | | METHOD | | | | | | | | | IMPACT | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access | Trust | | | | Motivation | Goal | Acts | | | | | Limits | | | | | | | | |
| | | None | Partial Trust | Employee | Administrator | | | Copy, Expose | Deny, Withhold, Ransom | Destroy, Delete, Render Unavailable | Damage, Alter | Take, Remove | Code of Conduct | Legal | Crimes Against Property | Crimes Against People | Loss of Financial Assets | Business Operations Impact | Loss of Competitive Advantage, Market Share | Legal or Regulatory Exposure | Degradation of Reputation, Image, or Brand |
| Employee Error | Internal | | X | X | X | Accidental/Mistake | No malicious intent, accidental | X | | X | X | | X | | | | X | X | X | X | X |
| Reckless Employee | Internal | | X | X | X | Accidental/Mistake | No malicious intent, accidental | X | | X | X | | | X | | | X | X | X | X | X |
| Information Partner | Internal | | X | | | Accidental/Mistake | No malicious intent, accidental | X | | X | X | | | | | | X | X | X | X | X |
| Competitor | External | X | | | | Personal Gain (Financial) | Obtain Business or Technical Advantage | X | | | | | | | X | | | | X | | |
| Radical Activist | External | X | | | | Social/Moral Gain | Change Public Opinion or Corporate Policy | X | X | X | X | X | | | | X | | X | | | X |
| Data Miner | External | X | | | | Personal Gain (Financial) | Obtain Business or Technical Advantage | X | | | | | | | X | | | | X | | |
| Vandal | External | X | | | | Personal Gain (Emotional) | Personal Recognition or Satisfaction | | | X | X | | | | X | | | X | | | X |
| Disgruntled Employee | Internal | | X | X | X | Personal Gain (Emotional) | Damage or Destroy Organization | | X | X | X | | | | X | | | X | X | | X |

http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf

# Threat Actors/Actions — TARA



| | Employee | Contractor | Privileged | Hacktivist | Competitor | Terrorist | Org Crime | Vendor | Gov't |
|---|---|---|---|---|---|---|---|---|---|
| Internal | ■ | ■ | ■ | | | | | | |
| External | | | | ■ | | | ■ | ■ | ■ |
| **Action(s)** | | | | | | | | | |
| Copy | ■ | ■ | ■ | | ■ | ■ | ■ | ■ | ■ |
| Deny | ■ | | ■ | | ■ | ■ | ■ | | |
| Destroy | ■ | | ■ | | | ■ | | | |
| Damage | ■ | | ■ | ■ | | ■ | | | ■ |
| Take | ■ | ■ | ■ | | | ■ | ■ | | |
| **Capability** | | | | | | | | | |
| VH | | | ■ | | | | ■ | | ■ |
| H | | | | | | ■ | | | |
| M | ■ | ■ | | | ■ | | | ■ | |
| L | | | | ■ | | | | | |
| VL | | | | | | | | | |

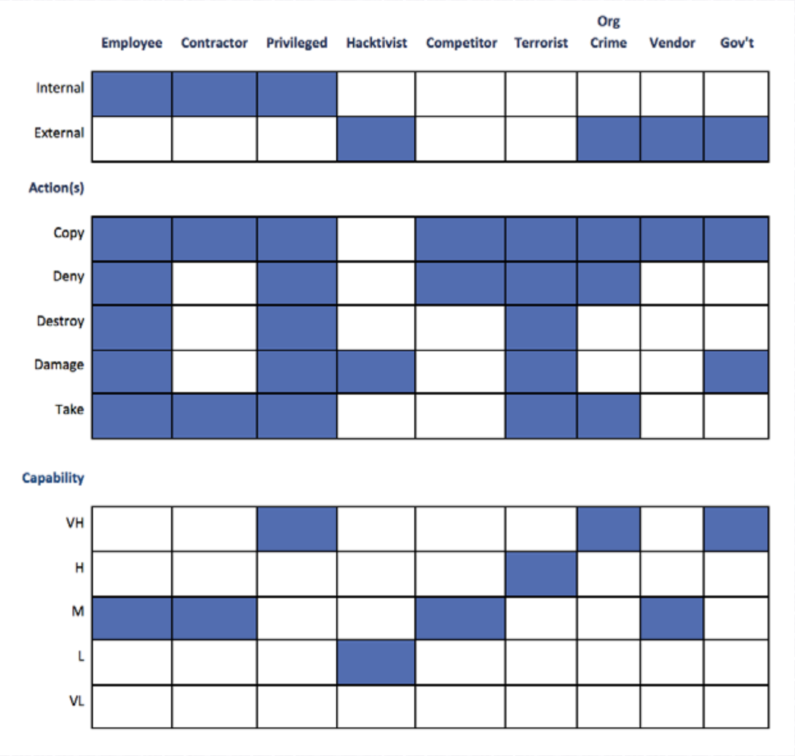
- Qualitative at a high level

http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf

# Threat Actors/Actions – Intelligence

- OSINT
  - “*bins”, GitHub, StackOverflow, etc. http://holisticinfosec.blogspot.com/search?q=osint
  - Google alerts, etc.
- *-ISACs info sharing
- Federal bulletins
- Services (e.g. RecordedFuture)

# Threat Actors/Actions — TARA



| | Employee | Contractor | Privileged | Hacktivist | Competitor | Terrorist | Org Crime | Vendor | Gov't |
|---|---|---|---|---|---|---|---|---|---|
| Internal | ■ | ■ | ■ | | | | | | |
| External | | | | ■ | | | ■ | ■ | ■ |
| **Action(s)** | | | | | | | | | |
| Copy | ■ | ■ | ■ | | ■ | ■ | ■ | ■ | ■ |
| Deny | ■ | | ■ | | ■ | ■ | ■ | | |
| Destroy | ■ | | ■ | | | ■ | | | |
| Damage | ■ | | ■ | ■ | | ■ | | | ■ |
| Take | ■ | ■ | ■ | | | ■ | ■ | | |
| **Capability** | | | | | | | | | |
| VH | | | ■ | | | | ■ | | ■ |
| H | | | | | | ■ | | | |
| M | ■ | ■ | | | ■ | | | ■ | |
| L | | | | ■ | | | | | |
| VL | | | | | | | | | |

- Qualitative at a high level
- Quantitative in discrete contexts (e.g. risk assessments)

*So, how you get #'s?*

http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf

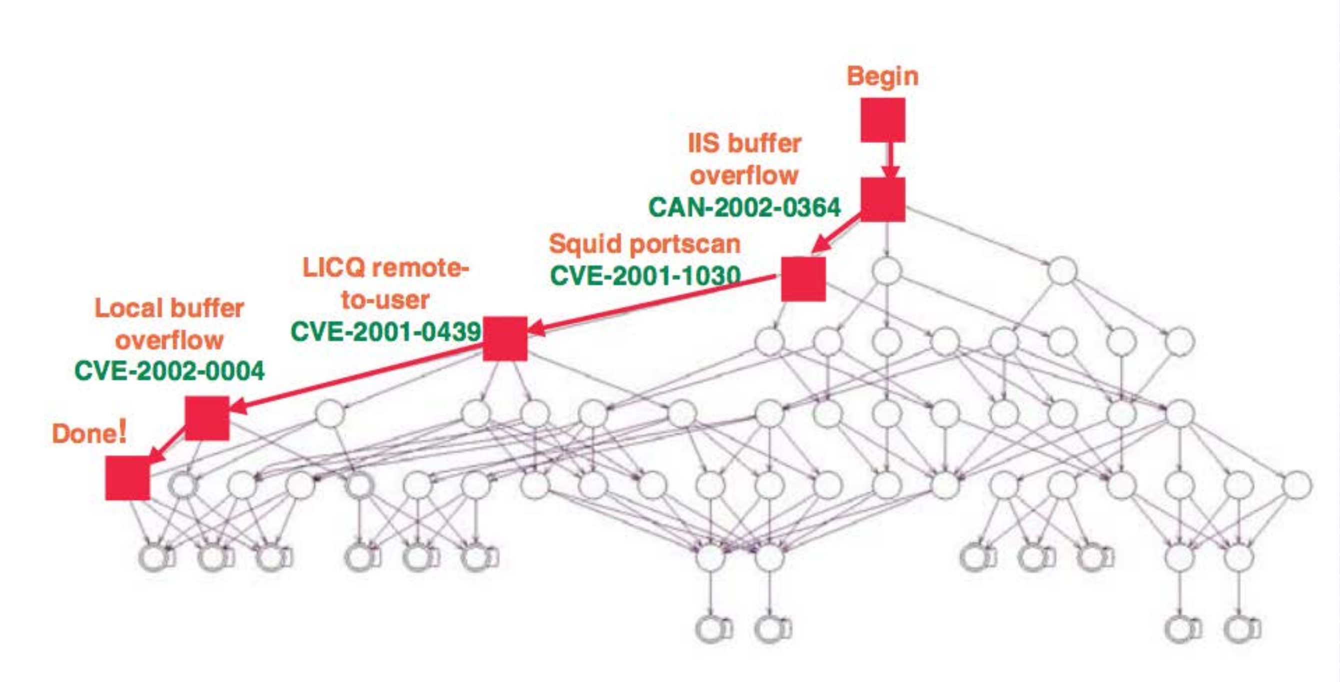
# Threat Actors/Actions – Events

- Your own incidents (phishing, virus hits, near misses) - simple counting! Don't hide!
- Your own breaches (disclosed or otherwise) - simple counting!
- Security industry sources (I’m kinda partial to the DBIR) - simple counting
- Vertical industry peers (back to the ISACs again) - simple counting!

Critical assets.

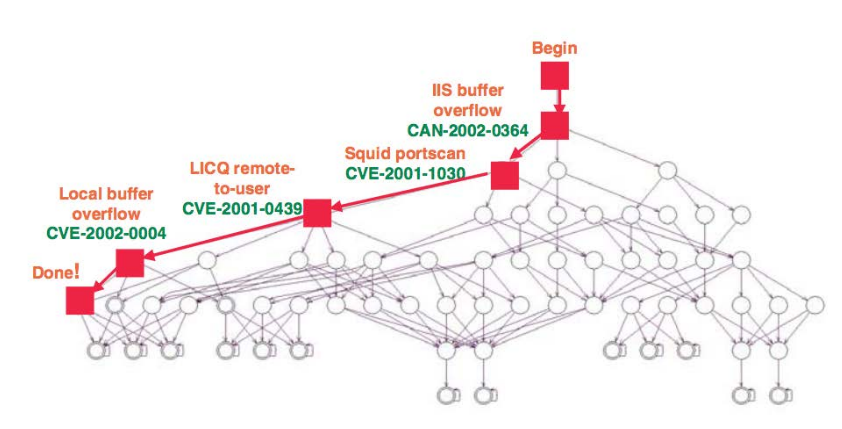
Control (Resistance) Strength.

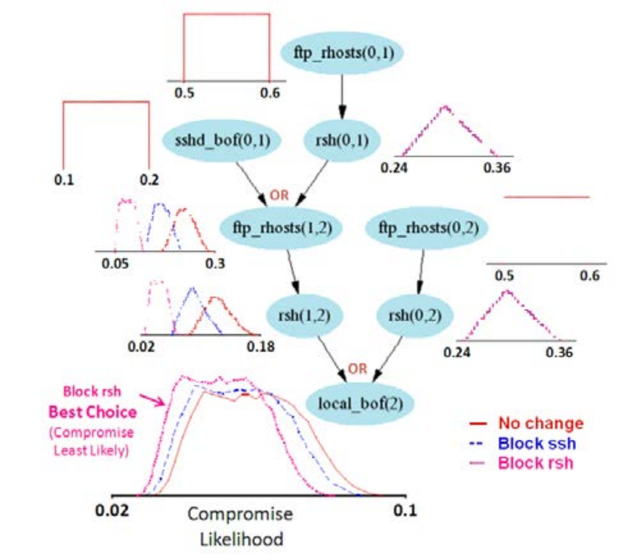
# Critical Assets & Control Strength



http://www.cs.cmu.edu/~wing/publications/SheynerWing04.pdf

# Critical Assets & Control Strength

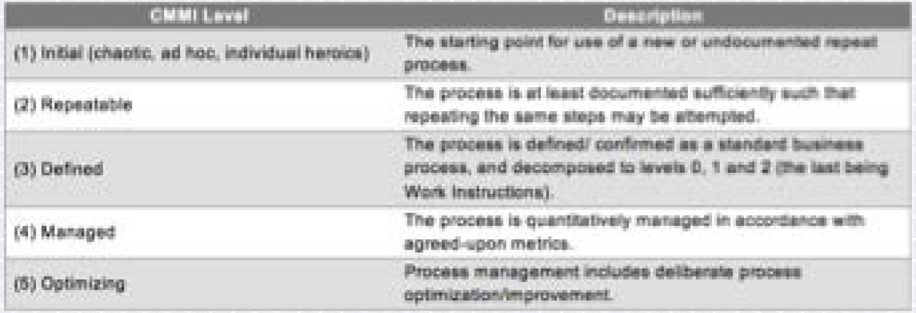




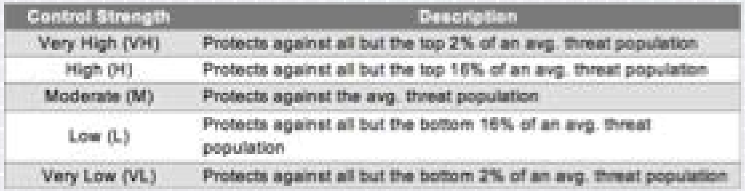
http://www.cs.cmu.edu/~wing/publications/SheynerWing04.pdf

http://csis.gmu.edu/noel/pubs/2010_IJNGC.pdf

# Critical Assets & Control Strength



| CMMI Level | Description |
|---|---|
| (1) Initial (chaotic, ad hoc, individual heroics) | The starting point for use of a new or undocumented repeat process. |
| (2) Repeatable | The process is at least documented sufficiently such that repeating the same steps may be attempted. |
| (3) Defined | The process is defined/ confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions). |
| (4) Managed | The process is quantitatively managed in accordance with agreed-upon metrics. |
| (5) Optimizing | Process management includes deliberate process optimization/improvement. |



| Control Strength | Description |
|---|---|
| Very High (VH) | Protects against all but the top 2% of an avg. threat population |
| High (H) | Protects against all but the top 16% of an avg. threat population |
| Moderate (M) | Protects against the avg. threat population |
| Low (L) | Protects against all but the bottom 16% of an avg. threat population |
| Very Low (VL) | Protects against all but the bottom 2% of an avg. threat population |

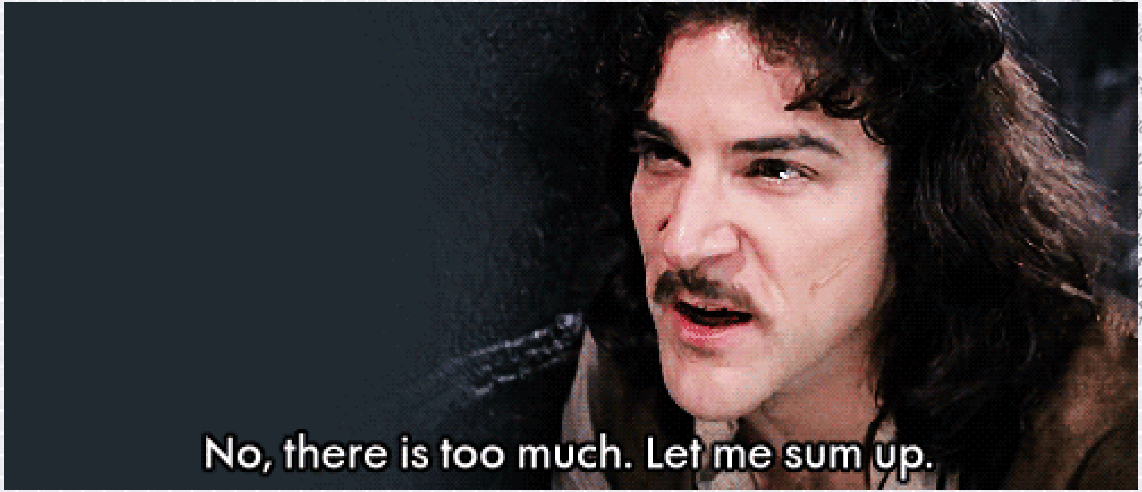
1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

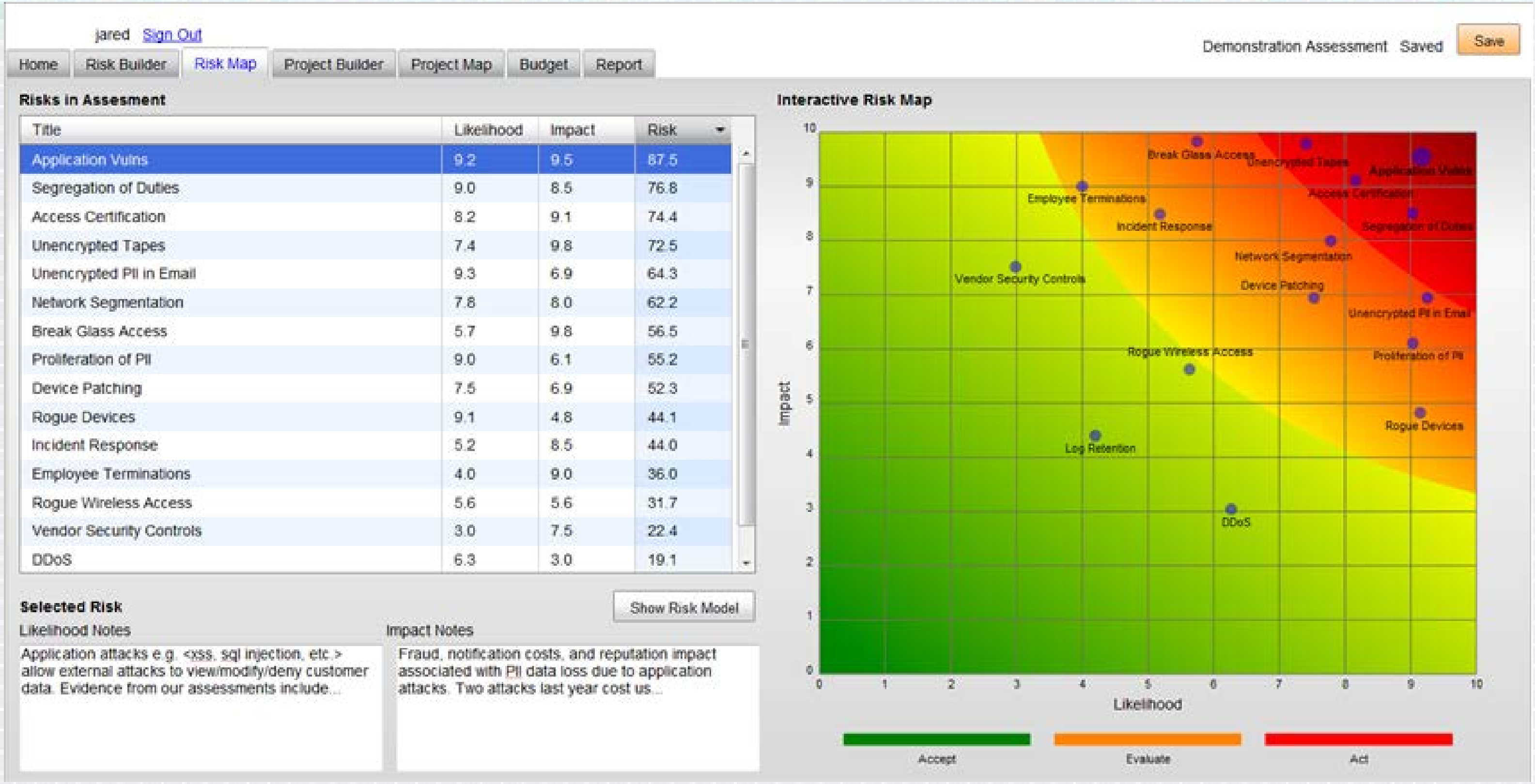
https://www.sans.org/media/critical-security-controls/CSC-5.pdf

# Impact.

# Incidents.

# Impact & Incidents


No, there is too much. Let me sum up.



**Risks in Assesment**

| Title | Likelihood | Impact | Risk |
|---|---|---|---|
| Application Vulns | 9.2 | 9.5 | 87.5 |
| Segregation of Duties | 9.0 | 8.5 | 76.8 |
| Access Certification | 8.2 | 9.1 | 74.4 |
| Unencrypted Tapes | 7.4 | 9.8 | 72.5 |
| Unencrypted PII in Email | 9.3 | 6.9 | 64.3 |
| Network Segmentation | 7.8 | 8.0 | 62.2 |
| Break Glass Access | 5.7 | 9.8 | 56.5 |
| Proliferation of PII | 9.0 | 6.1 | 55.2 |
| Device Patching | 7.5 | 6.9 | 52.3 |
| Rogue Devices | 9.1 | 4.8 | 44.1 |
| Incident Response | 5.2 | 8.5 | 44.0 |
| Employee Terminations | 4.0 | 9.0 | 36.0 |
| Rogue Wireless Access | 5.6 | 5.6 | 31.7 |
| Vendor Security Controls | 3.0 | 7.5 | 22.4 |
| DDoS | 6.3 | 3.0 | 19.1 |

**Selected Risk**

Likelihood Notes

Application attacks e.g. <xss, sql injection, etc.> allow external attacks to view/modify/deny customer data. Evidence from our assessments include...

Impact Notes

Fraud, notification costs, and reputation impact associated with PII data loss due to application attacks. Two attacks last year cost us...

**Interactive Risk Map**

http://www.calibersecurity.com/

## *What Should We Do To Reduce Risk?*

NAC!

# *What Should We Do To Reduce Risk?*

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

# *Outside In:*

## Building A Data-Driven Security Risk Management Program

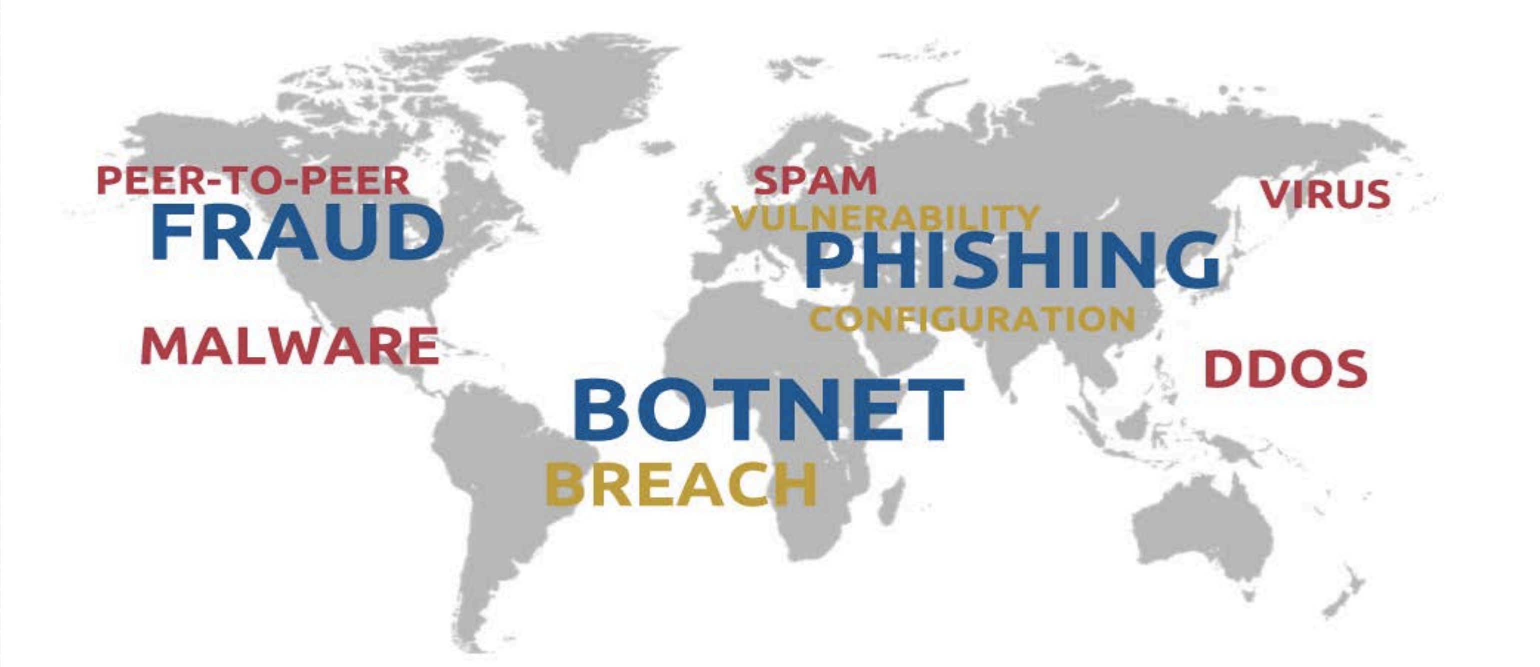
# “Are *We* Secure?!”

- Board of Directors
- Senior Leadership
- General Council
- Internal Stakeholders

- Customers
- Patients
- Partners
- Investments / M&A

## “Are ***<u>You</u>*** Secure?!”

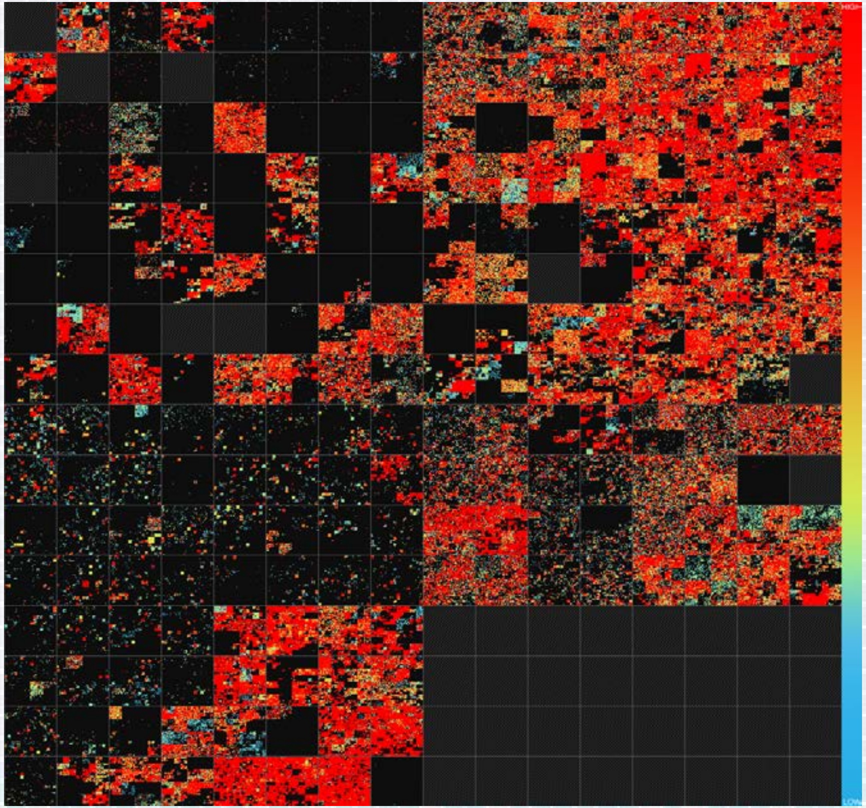
# Outside In: In Search of Controls Effectiveness



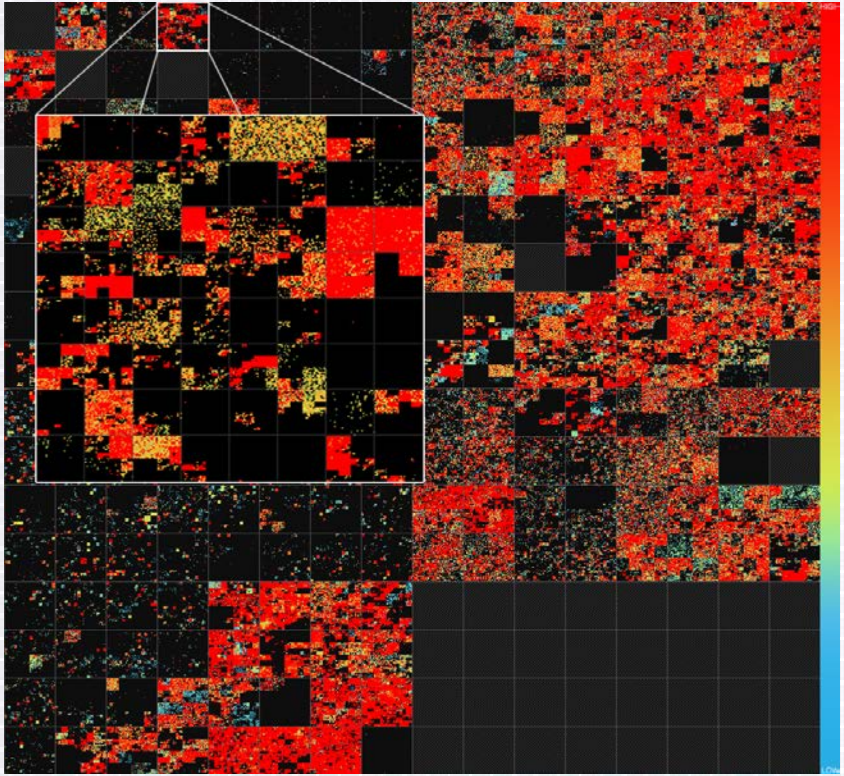
- System compromise
- Configurations
- User Behaviors

# Global View: Public IPv4 Space

- Measureing all 4.3 billion public addressesof Directors
- Colored dots represent behavioral observations
- Clear organizational differences
- Behavior changes over time



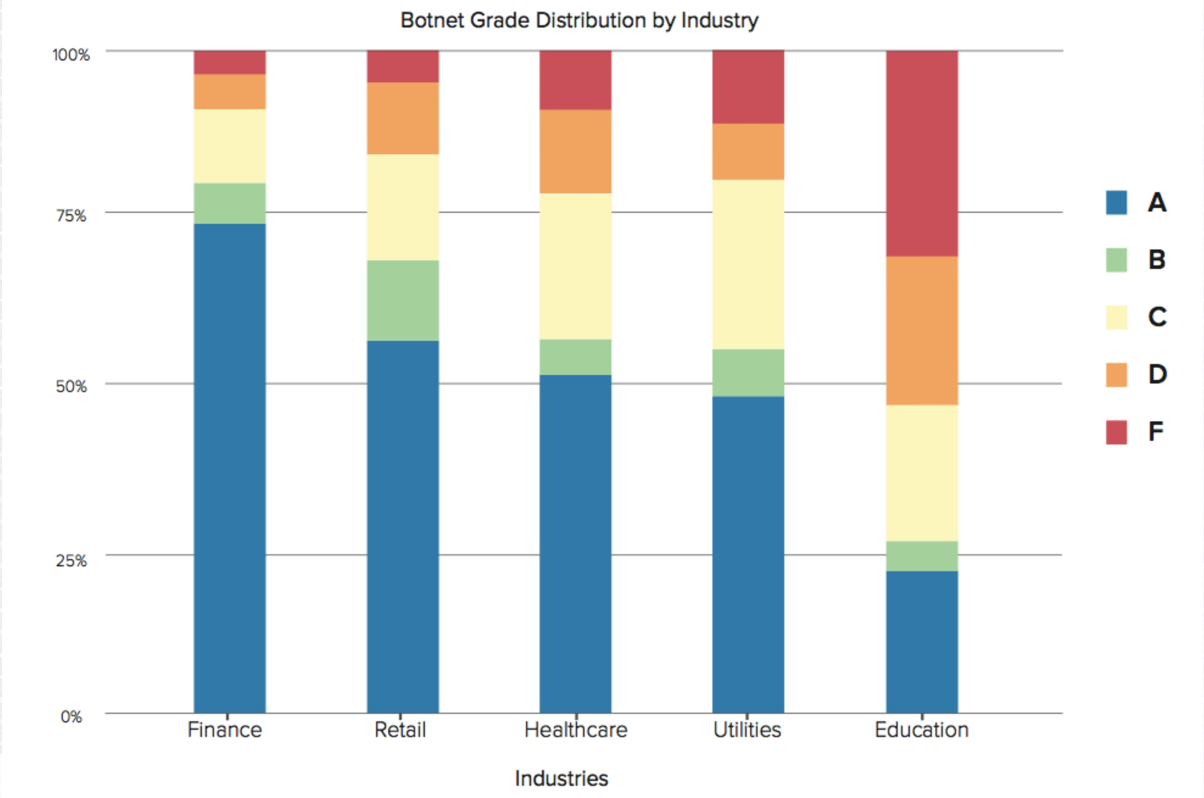
# Global View: Entity Level Focus (5.0.0.0/8)



- Over **860 entities** representing multiple industries
  - Electronic Arts
  - Apple
  - Fedex
  - News Corp
  - Walmart
  - Pepsi
  - Aon
  - Amgen
  - Priceline

Notes: Outcomes differ by entity

# Industry Observable System Compromises



- Grades consider the following:
  - Frequency
  - Duration
  - Severity

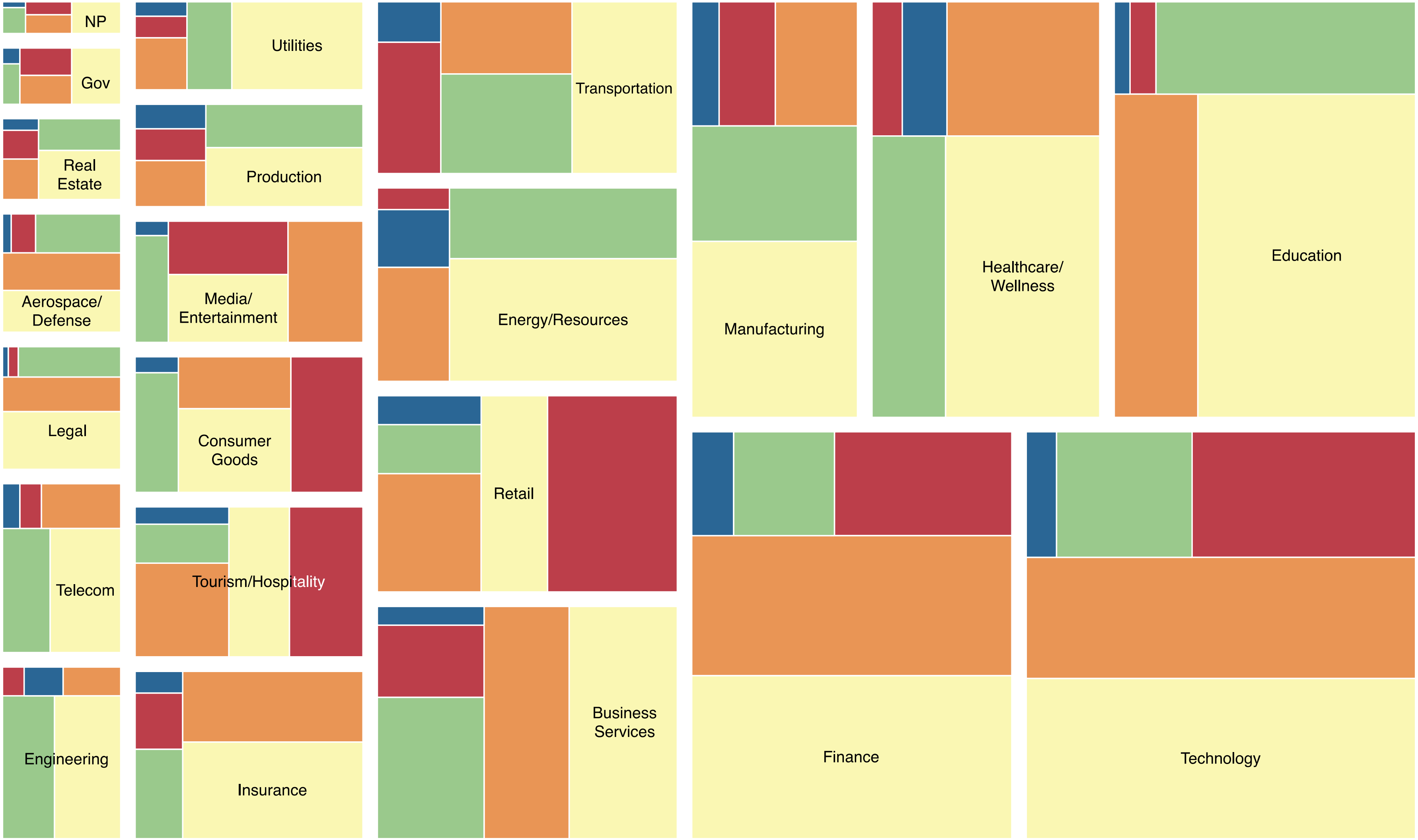
- Better performing organizations of ***fewer*** infections for ***shorter*** durations

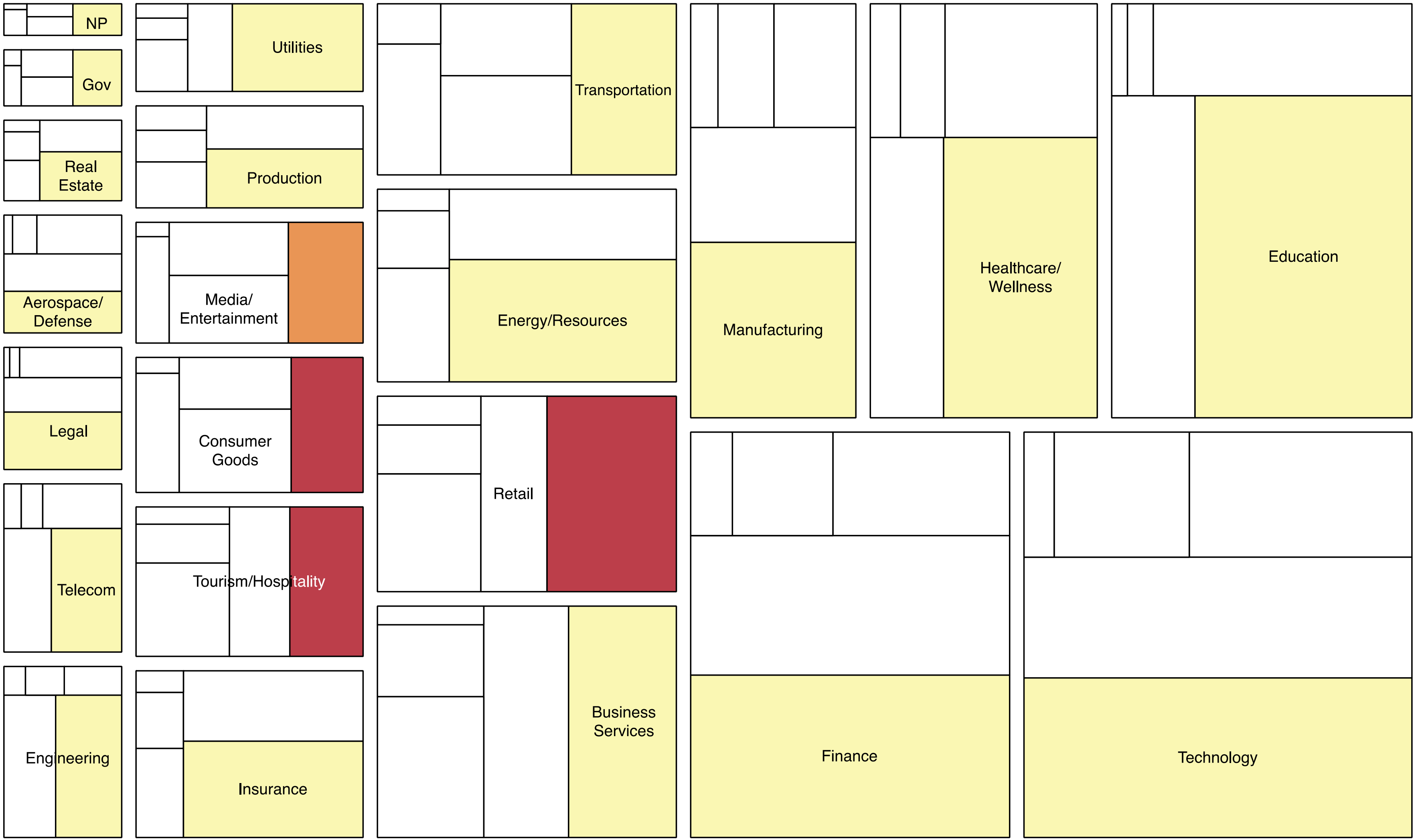
verizon BITSIGHT

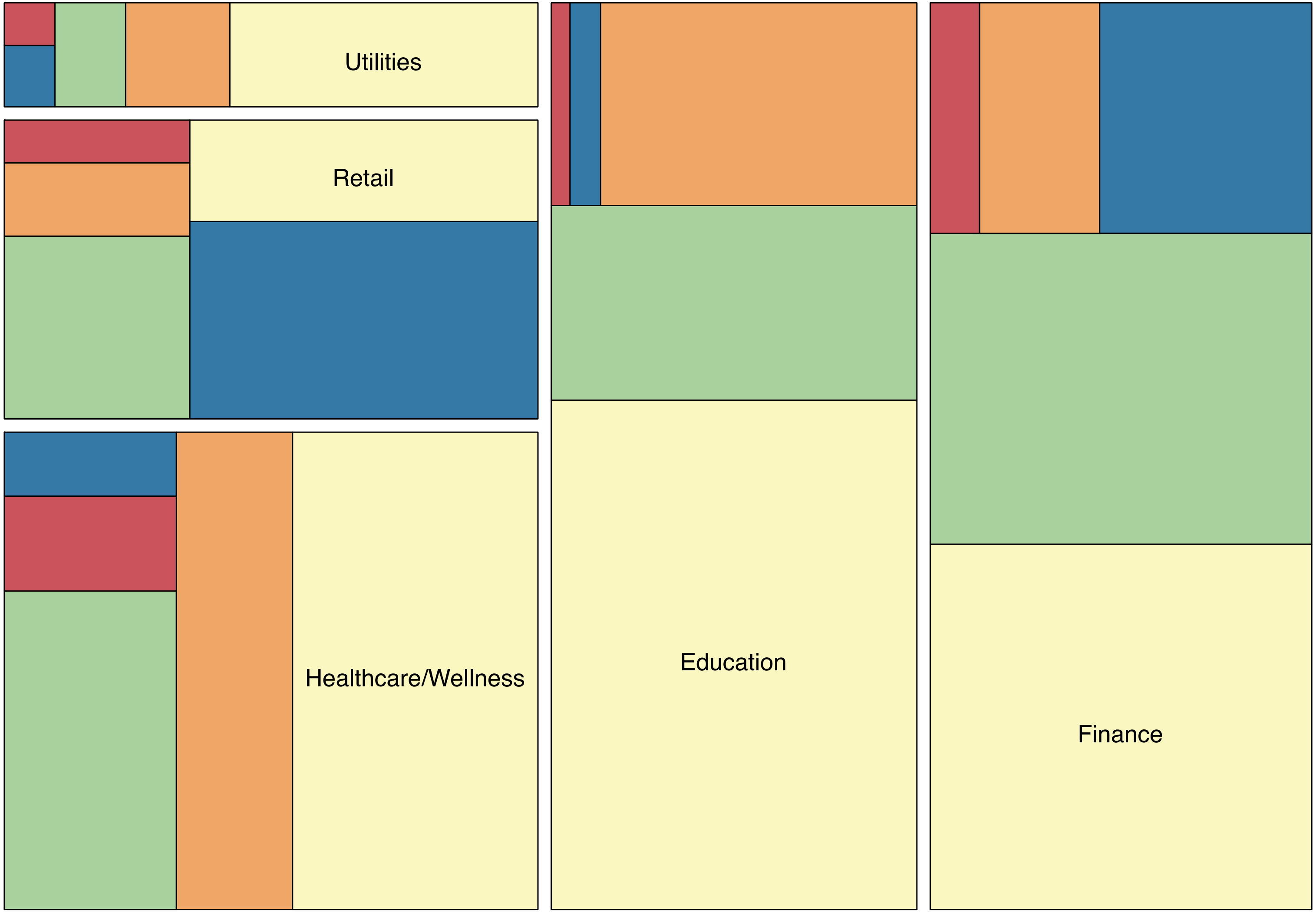
# A Look At TLS/SSL By Industry

- Grades consider the following:
  - Cypher Support
  - Protocol Support
  - Cert. status
  - Vulnerability

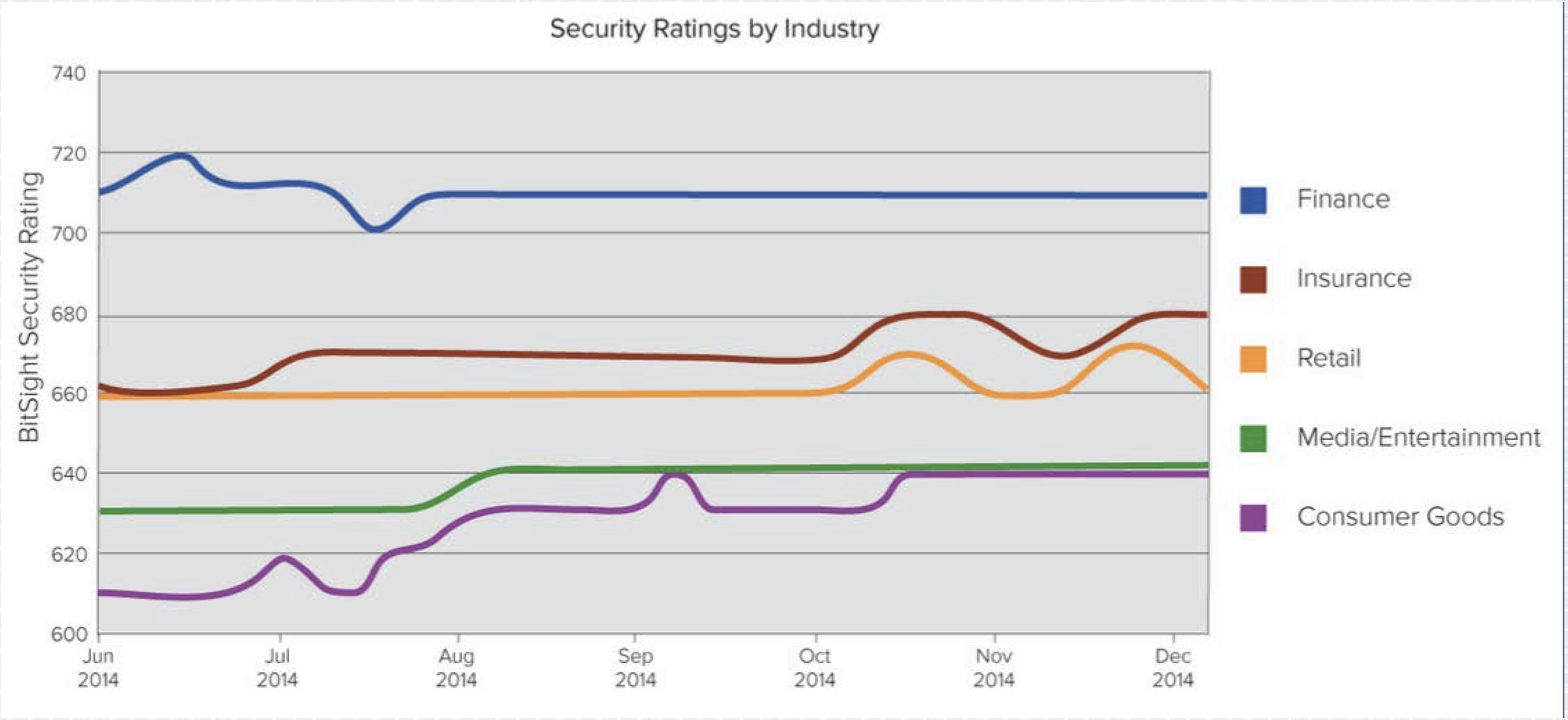
- Better performing organizations of ***fewer* bad** grades meaning ***better*** configuration management


NP
Gov
Real Estate
Aerospace/ Defense
Legal
Telecom
Engineering
Utilities
Production
Media/ Entertainment
Consumer Goods
Tourism/Hospitality
Insurance
Transportation
Energy/Resources
Retail
Business Services
Manufacturing
Healthcare/ Wellness
Education
Finance
Technology


NP
Gov
Real Estate
Aerospace/ Defense
Legal
Telecom
Engineering
Utilities
Production
Media/ Entertainment
Consumer Goods
Tourism/Hospitality
Insurance
Transportation
Energy/Resources
Retail
Business Services
Manufacturing
Healthcare/ Wellness
Education
Finance
Technology


Utilities
Retail
Healthcare/Wellness
Education
Finance

# Industry Ratings Comparison



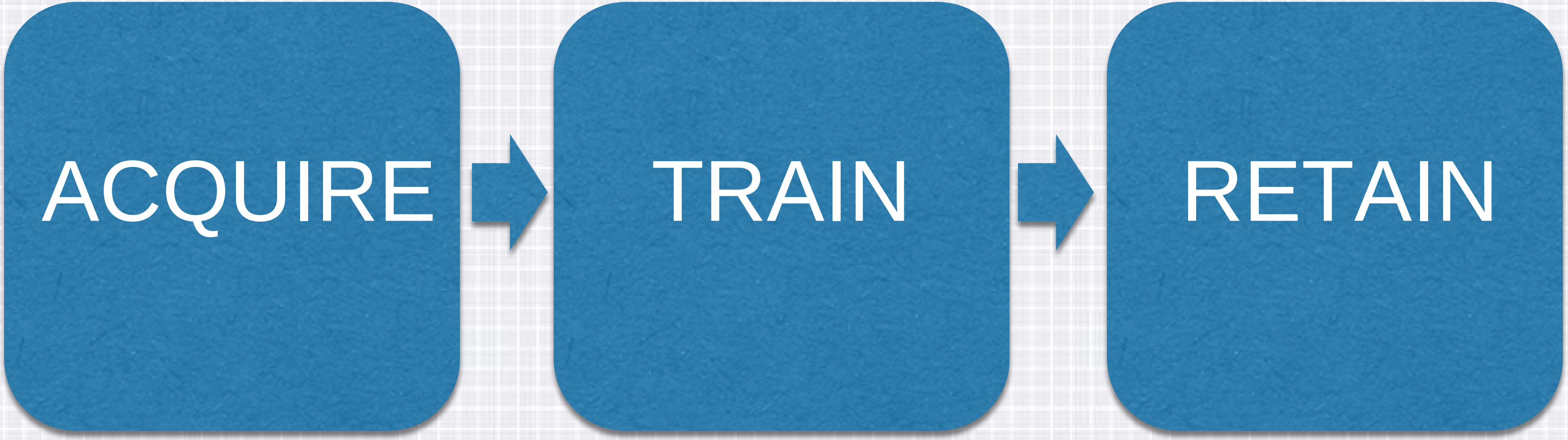
# Practical Application: Outside In Case Study

- **Profile**:
  - Global Vitamin and Nutritional Supplement Manufacturing
  - $3B+ annual revenue
- **Challenges**:
  - Lacked comparative data against industry peers
  - Need tools to communicate performance to management
  - Limited visibility into the supply chain partners
- **Results**
  - Weekly reports to executive management
  - Prioritization of internal initiatives
  - Requiring additional penetration testing and cyber insurance coverage of vendors
  - A “metric of pride” for the security group

*Sounds great but..*

*What is going to do this?*

# Attracting Talent



ACQUIRE

TRAIN

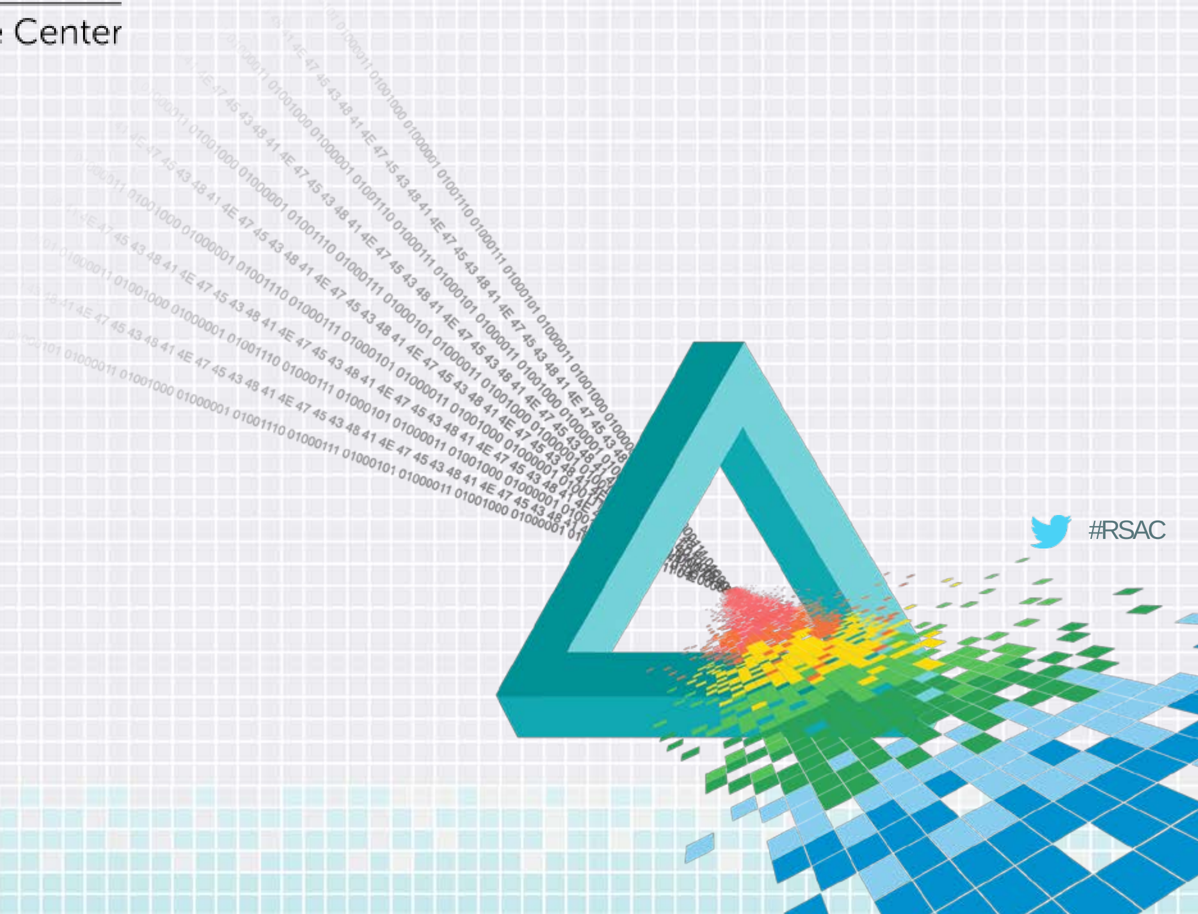
RETAIN

# Summary and Application

- Evolution of security towards **Data Driven Risk Management**
- Risk management begins the **Measurement**
- Measurement approaches to building a Data Driven Security Risk Management Program
  - **Inside Out**
  - **Outside in**
- Execution requires commitment and **Talent**
  - Consider grooming from alternative disciplines

RSAConference2015

San Francisco | April 20-24 | Moscone Center



# QUESTIONS?