

# A Wake-Up Call?

*Fight Back Against Cybercrime*

Prepared for:

## Information Security Forum

For Texas Government

Austin, Texas

May 20, 2015



IT Governance, Risk & Compliance

**Ricky Link**  
**Managing Director, Southwest**  
**Coalfire Systems, Inc.**

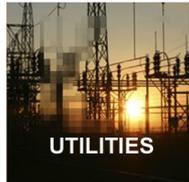
# Coalfire Background

- **Leading Information Security Advisory Consulting Firm**  
Offices: Atlanta, Dallas, Denver, New York, San Diego, San Francisco, Seattle, Washington DC, London



- **Customers Served**

10,000+ Engagements: 3PAO, FISMA, DIACAP, ICD 503, GLBA, SSAE 16, PCI, HIPAA, HITRUST, more



- **Sample Clients**



# Agenda

- A Wake-Up Call – What Went Wrong?
- Cyber Risk is Nothing New
- What Went Wrong with Breaches
- The Blueprint of An Attack – An Example
- Enough is Enough!
- FISMA – Annual Report to Congress
- Compliance Does Not Equal Security – Just a Baseline
- Questions



# A Wake-Up Call – The Cyber Threat is Increasing

## ■ Recent Cyber Attacks

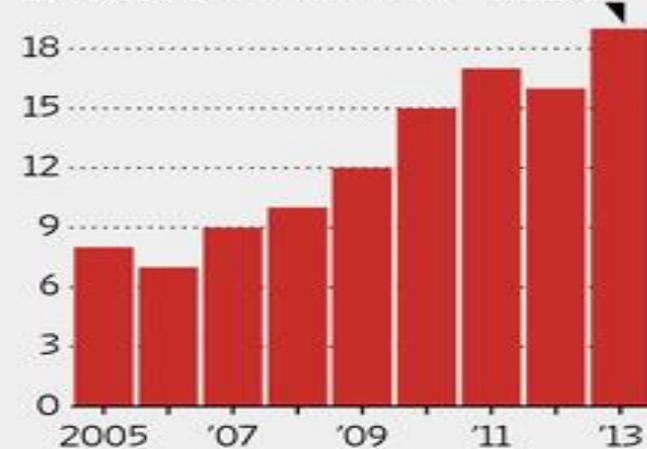
- » Major retailers are routinely targeted
- » Number of confirmed compromised credit cards range from 40-80 million cards
- » Combination of malware, memory-scraping programs, poor security controls used to remove sensitive data on a never before seen scale
- » Security programs were **validated** as “compliant”; however, were not operating effectively

## ■ Law Enforcement Warnings

- » Threats increasing on POS platforms and recent attacks are part of a larger scheme to defraud POS systems
- » Malware increasingly available at a price to make cybercrime achievable for novices

## Security Failures

The number of North American retailers in a Ponemon Institute study that experienced a data breach involving 5,000 or more customer records, by fiscal year



Note: Surveys of 55-66 retailers with at least 1,000 employees.  
Source: Ponemon Institute  
The Wall Street Journal



# A Wake-Up Call – Cyber Risk is Nothing New

## Coalfire Daily Media Report 5/7/15

- **Is Your Company Ready for a Cyber Attack? (Hint: Nope)**
- Outlet: PC Magazine
- Link: <http://www.pcmag.com/article2/0,2817,2481346,00.asp>
- Snippet: Hackers are getting craftier and more specific, while companies struggle to keep up, Symantec found.

## Coalfire Daily Media Report 5/7/15

- **Half of US Health Care Providers Have Been Hacked**
- Outlet: Yahoo! Tech
- Link: <https://www.yahoo.com/tech/report-half-of-us-healthcare-providers-have-been-118323228724.html>
- Snippet: Cybercrooks have developed an unhealthy interest in your medical records, and the prognosis isn't good.



# A Wake-Up Call – Cyber Risk is Nothing New

## Coalfire Daily Media Report 5/6/15

### ■ **IT Pros Lack Confidence in Cyber-Defenses**

- Outlet: eWeek
- Link: <http://www.eweek.com/small-business/it-pros-lack-confidence-in-cyber-defenses.html>
- Snippet: Just 15 percent of companies surveyed believe their employees are "well prepared" to spot the signs of an attack and react accordingly.

## Coalfire Daily Media Report 4/29/15

### ■ **Survey: C-level Tech Execs Most Responsible for Breaches**

- Outlet: Info Security
- Link: <http://www.infosecurity-magazine.com/news/c-level-tech-exec-s-most/>
- Snippet: As the data breach epidemic rages on, the question of corporate liability has been front and center. It turns out that many security-industry folks believe that C-level technology executives would and should be the ones held responsible for compromises, new research has revealed.



# A Wake-Up Call – Cyber Risk is Nothing New

## Coalfire Daily Media Report 4/29/15

- **DOJ Provides Cybersecurity Info for Breach Victims**
- Outlet: The Wall Street Journal
- Link: <http://blogs.wsj.com/riskandcompliance/2015/04/29/doj-releases-cybersecurity-guidance-for-breach-victims/>
- Snippet: The US DOJ, as part of a broader roll out of its engagement with the corporate sector on cyber issues, released guidance containing what it sees as best practice for victims — and potential victims — of data breaches.

## Coalfire Daily Media Report 4/13/15

- **President Issues Third Cybersecurity Exec Order In 2 Years**
- Outlet: The National Law Review
- Link: <http://www.natlawreview.com/article/president-issues-third-cybersecurity-executive-order-two-years>
- Snippet: President Obama issues EO for Economic Sanctions to Deter Those Who Target US Critical Infrastructure Using “Significant Malicious Cyber Related Activities”.



# What Went Wrong with US Breaches?

Security operations excellence matters...

- Computer anti-virus protection was not working or ineffective
- Egress filtering was not set to limit exfiltration of stolen data
- Lack of two-factor administrative access authentication
- No file integrity monitoring or application white listing to prevent malware installation
- Ineffective security monitoring and alerting



# The Blueprint for Attacks

All recent payment card breaches share similar and critical steps that hackers apply over and over...

## 1. Getting Access to the critical data including PII

- Getting exploits, malware and tools in

## 2. Harvesting Sensitive Data

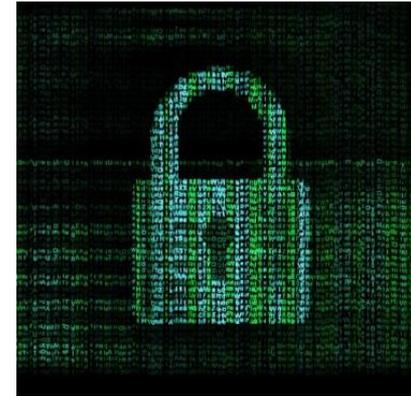
- Gathering sensitive data (track data for example) from unprotected repositories or memory

## 3. Propagation Across Environment

- Spreading the malware around, infect all possible locations

## 4. Getting your data out

- Moving large amounts of valuable data to external systems

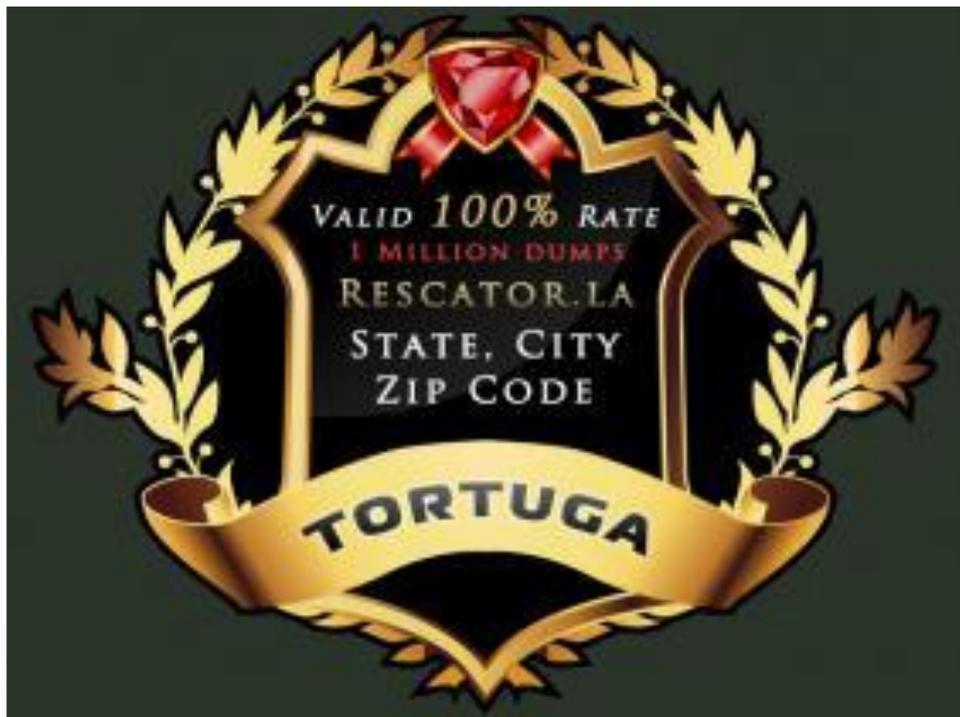


**<<DEFENSE IN DEPTH>>**



# Analysis of 2013 Merchant Breach

## Advertisement for Stolen Credit Cards



*Source: [Krebsonsecurity.com](http://Krebsonsecurity.com)*

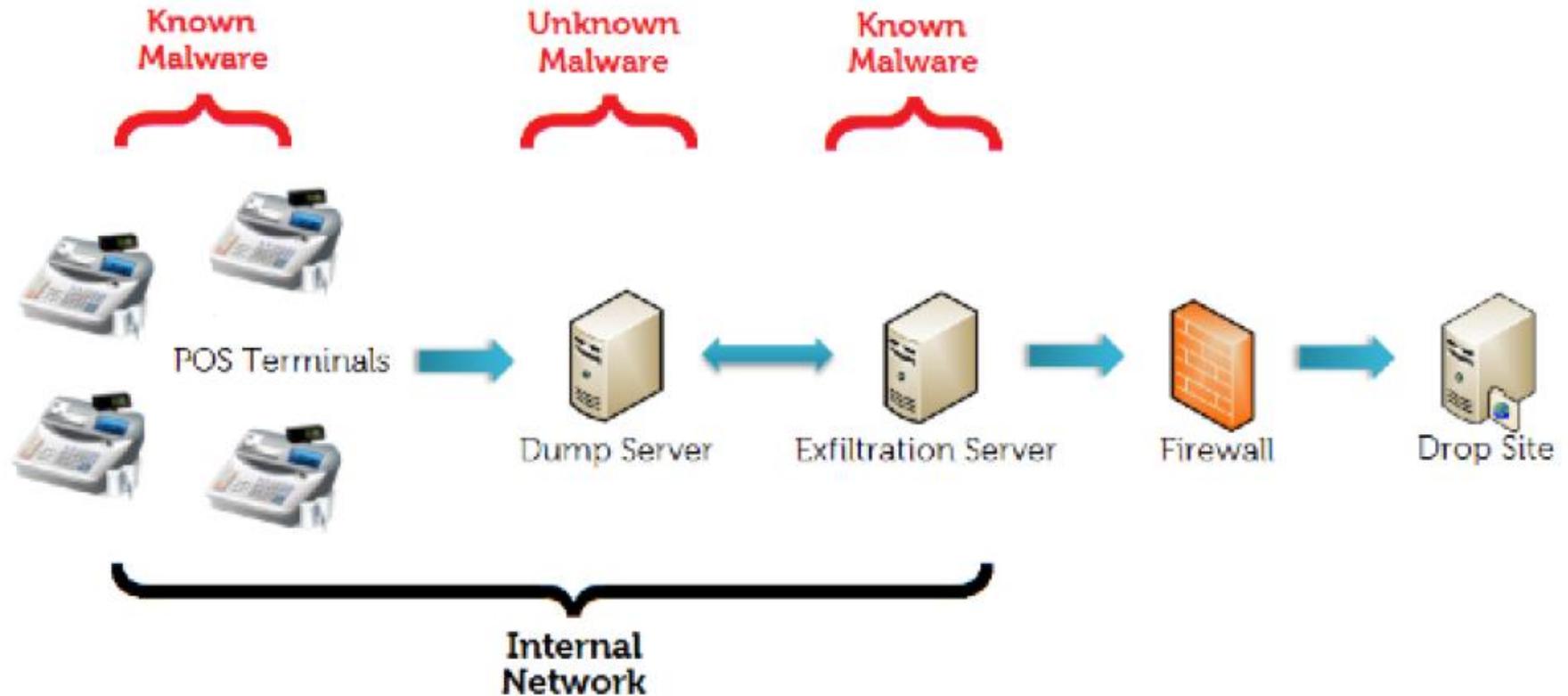
Source: Committee on Commerce, Science & Transportation

"A "Kill Chain" Analysis of the 2013 Data Breach" report dated 3/26/14



# Analysis of 2013 Merchant Breach

## Diagram of an Data Exfiltration



Source: Committee on Commerce, Science & Transportation

“A “Kill Chain” Analysis of the 2013 Data Breach” report dated 3/26/14



# Defense in Depth

**Defense in Depth** may have prevented or limited the scope of this disaster. An attacker may have the time and resources to circumvent 1 or 2 security controls; however, a strong security program with multiple layers of security may have stopped this attack in any of the four critical steps. Let's look at some critical security controls and how they may have prevented an attack:



**Network Segmentation (inbound and outbound):** Strong access controls lists on firewalls and routers should always be implemented to restrict access both to and from sensitive networks. **Prevented Steps: Getting In, Propagation, Getting Out**

**Logical Access Controls:** How was access to the corporate environment, CHD and connected systems managed? Domain controllers are a common compromise point for all organizations. **Prevented Steps: Getting In, Propagation, Getting Out**

**Vendor Due Diligence:** The need to monitor the security status of third-party vendors and ensuring vendor access is being used in its intended manner is critical. **Prevented Steps: Getting In**

# Defense in Depth (ii)



**Anti-Virus and File-Integrity Monitoring (FIM):** These technologies can prevent malware and other malicious software from being placed on critical systems. The alerts from these technologies could prevent a minor compromise from becoming a major disaster.

**Prevented Steps: Harvesting, Propagation**

**Logging, Monitoring and Alerting:** Absolutely the most critical of all security layers and the biggest misstep for preventing the recent attacks. Security events and logs from all security layers must be logged and monitored at all times. Failing to act upon these alerts renders these technologies completely useless.

**Prevented Steps: Getting In, Harvesting, Propagation, Getting Out**

**Two-Factor Access:** Technologies that go beyond the traditional “Username/Password” requirements are considered best practice for controlling access into sensitive areas including the cardholder data environment. These shouldn’t be seen as applicable for remote Internet access only.

**Prevented Steps: Getting In, Getting Out**

**Data Protection:** Encrypting, tokenizing or altering sensitive data reduces or eliminates the value of this data throughout an environment. Point-of-Interaction technologies such as E2EE, P2PE and tokenization will mitigate the damage should a defense in depth program fail at any single point.

**Prevented Steps: Harvesting**



# Enough is Enough

- Time for fresh ideas and decisive action
- Comprehensive risk management
  - » Expanded Risk Assessment
    - Personally Identifiable Information (PII)
    - Intellectual Property
    - Operational Data
  - » Justified Response
    - Understand inherent risk
    - Mitigate risk to a justified level



# Cyber Risk is Nothing New

- Past data breaches are now an everyday occurrence
- What about recent cyber guidance
- Focus has escalated; consumers demand action
- More regulations...
- Another difficult decision...



# Annual Report to Congress:

## Federal Information Security Management Act 2002 (Feb 2015)

Filed annually by Office of Management and Budget (OMB) on the implementation status of all Federal agencies of FISMA.

1. Provides an update of ongoing information security initiatives.
2. Review of Fiscal Year 2014 information incidents.
3. Inspector General assessments of agencies' progress in implementing information security capabilities..
4. Federal Government's progress in meeting key information security performance measures based on agency submitted data.



# Annual Report to Congress:

Federal Information Security Management Act 2002 (Feb 2015)

## Key Report Sections

- Section I: Strengthening Federal Cybersecurity
- Section II: State of Federal Cybersecurity
- Section III: Summary of Inspectors General's Findings
- Section IV: Progress in Meeting Key Privacy Performance Measures

Source: [https://www.whitehouse.gov/sites/default/files/omb/assets/egov\\_docs/final\\_fy14\\_fisma\\_report\\_02\\_27\\_2015.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf)

# Multiple Control Models and Controls



SSAE 16 SOC 1/2



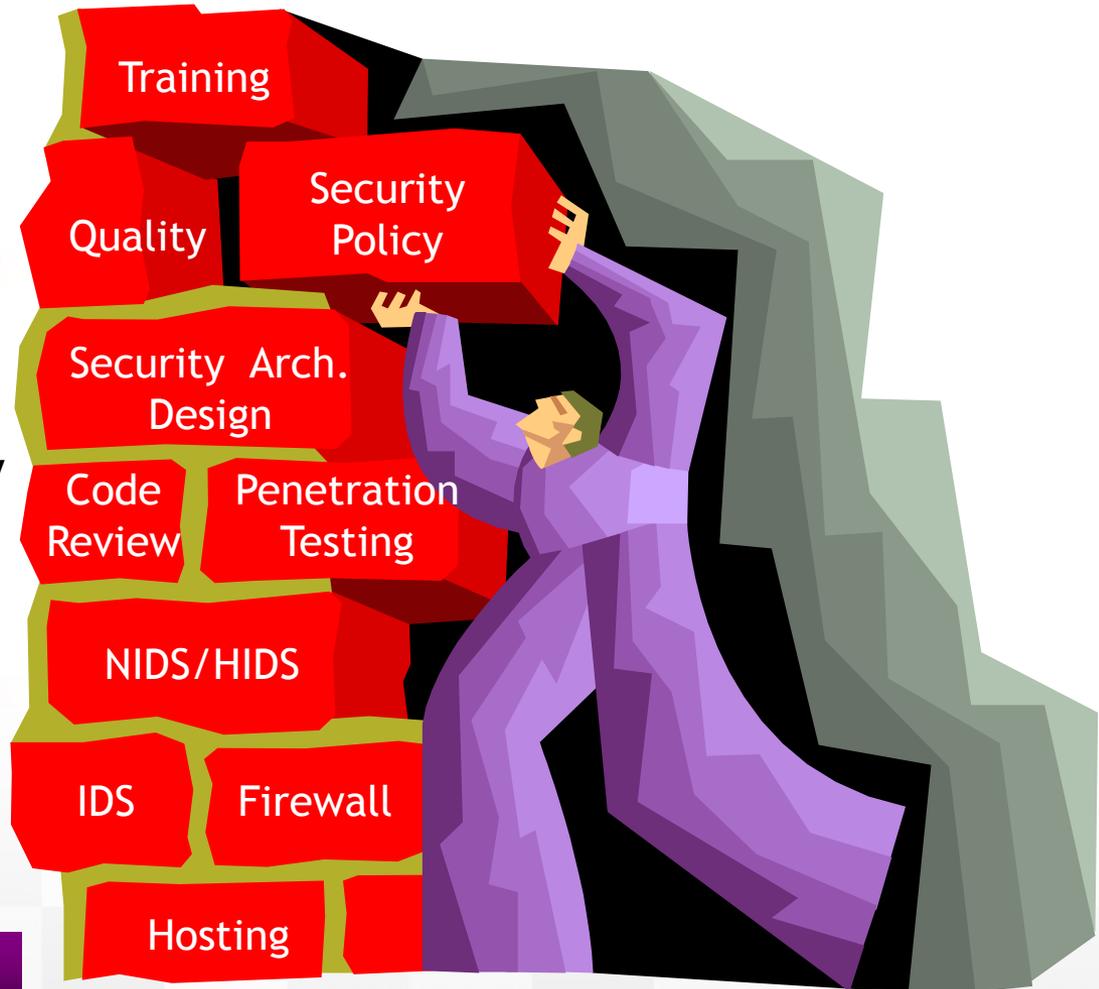
Texas Medical Privacy Act of 2012

ISO-27001/2

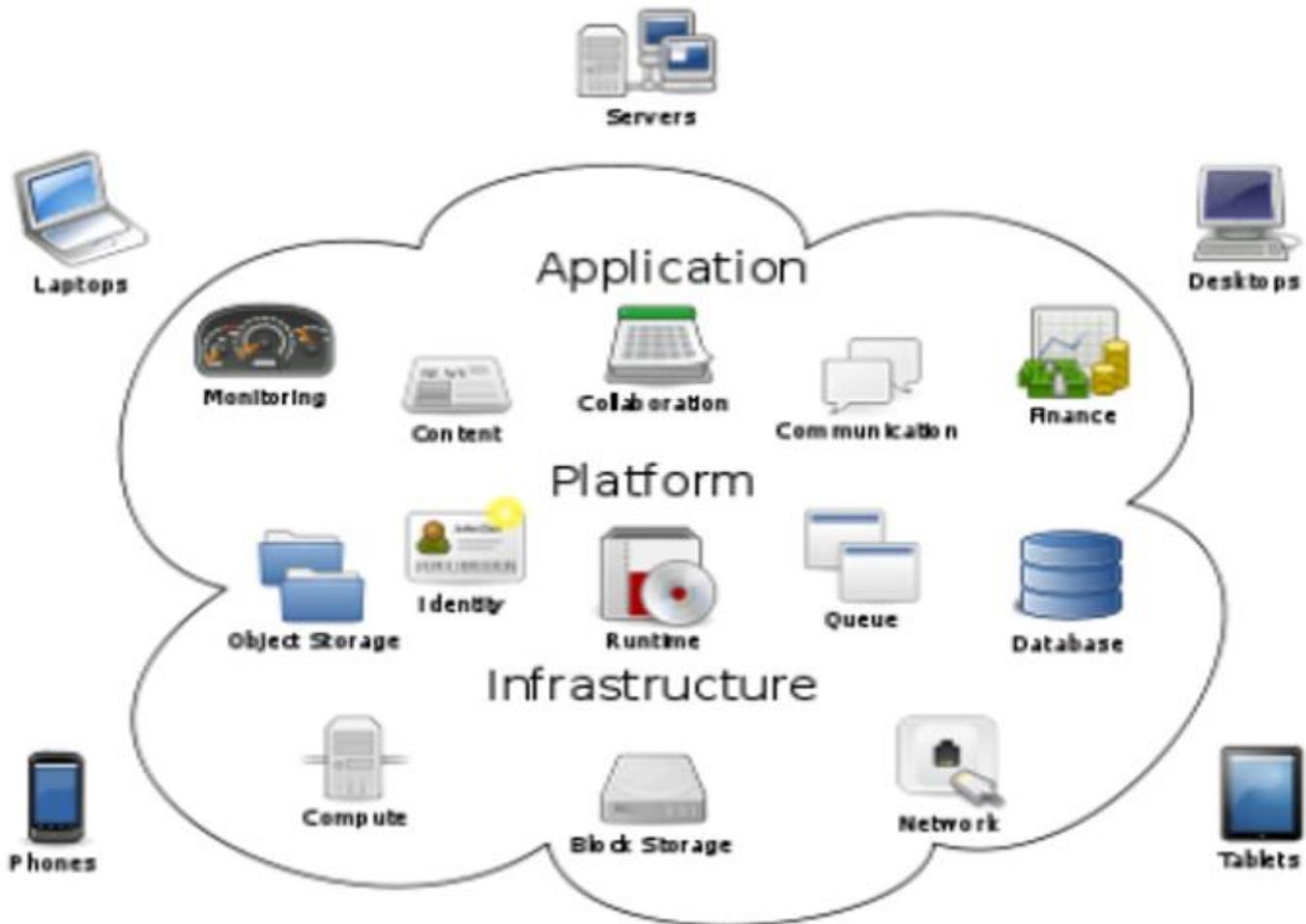
Privacy Laws



Information Security Forum for Texas Government

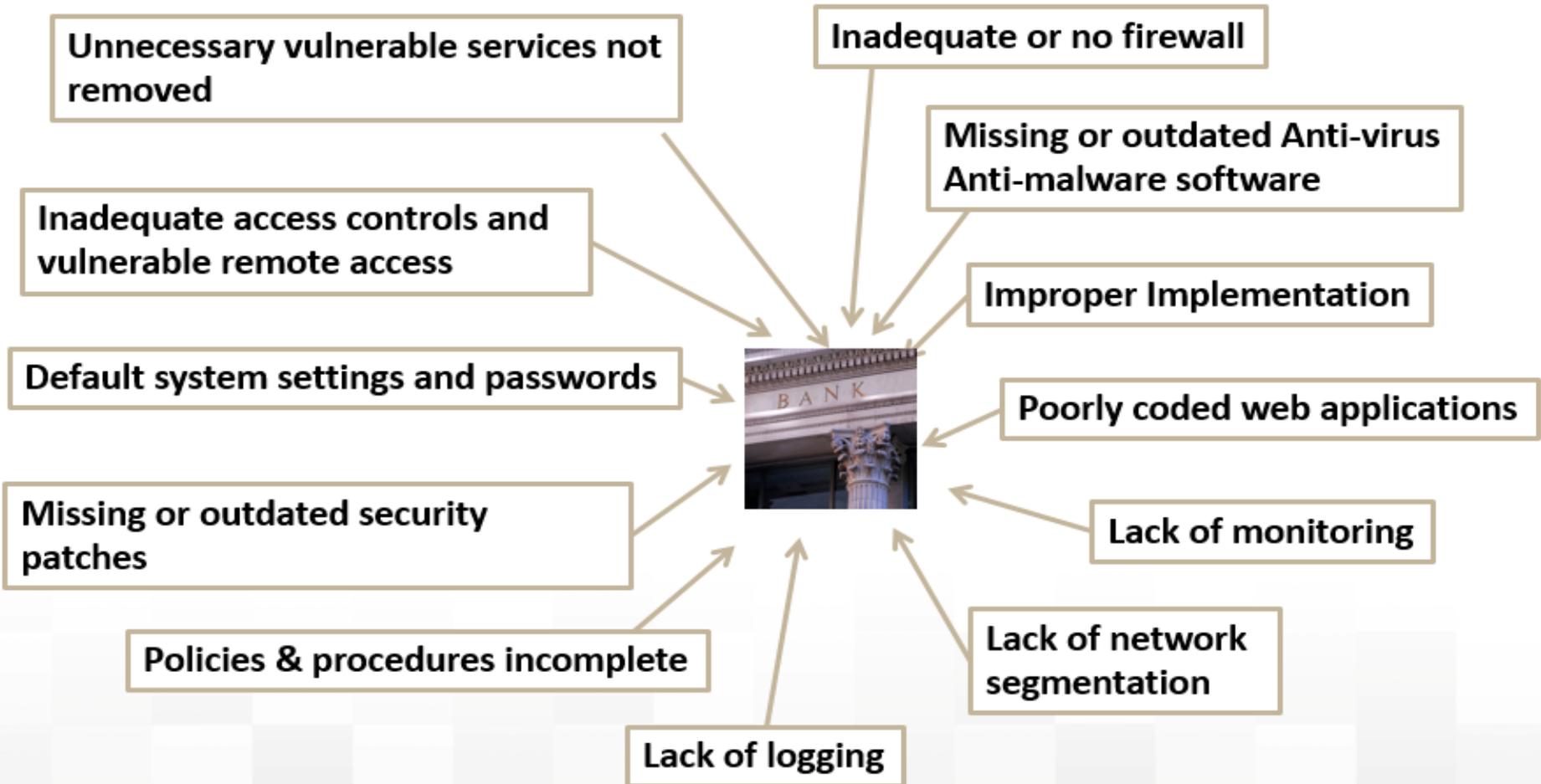


# Where did the Firewall Go?



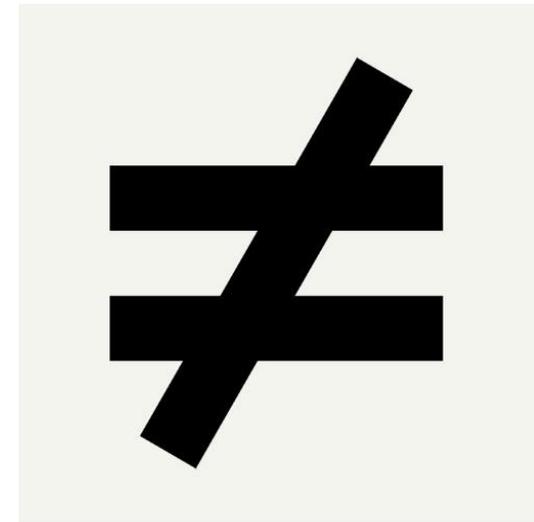
Cloud Environment

# Orgs Tend to Over-Estimate Their Compliance



# Compliance Does Not Equal Security

- The focus on information security still should be the basic blocking and tackling issues
- There is NO guaranteed protection
- Compliance is an outcome of an effective security program



# Compliance is Just a Baseline

- Compliance is a good start; however, much more is needed
- Another factor to consider is applicable Federal and State consumer data privacy laws
- Technology is great; however, beware as it is No Silver Bullet...
- The cloud provides a path to outsource functions; however, not the risk



# Beyond Compliance



- Defense in Depth
  - ✓ Physical and logical access controls
  - ✓ Sufficient network segmentation
  - ✓ File Integrity Monitoring (FIM) solution
  - ✓ Security Event and Incident Management (SEIM) solution
  - ✓ Encryption and/or tokenization
- Risk Management
  - ✓ Identify all critical assets
  - ✓ Prioritize criticality
  - ✓ Select controls
  - ✓ Establish effective oversight and governance



# A New Generation of Risk Management is Justified

- **Short-term actions – Am I already hacked?**
  - » Conduct a forensic analysis
  - » Take a second look at the top 5 critical controls in payment systems
    - Payment Application Data Security Standards validation and implementation
    - Network segmentation
    - Secure configuration management
    - Physical security
    - Logging, monitoring and alerting
- **Long-term actions – How do I stay off the front page of the *Wall Street Journal*?**
  - » Make IT GRC a top priority
  - » Explore risk-reducing technologies at the point of interaction



# Summary – The Data Security Risk is Significant & Therefore Requires Appropriate Controls

- The threat of data compromise is global in scope (Web)
- Many parties are involved in maintaining data security
- The impact of data compromise is widespread financially, legally, and in goodwill exposures
- Data security is a primary risk concern for companies, service providers, vendor, consumers, and regulators
- Data security has evolved from an operational problem and financial threat to a significant reputation risk

**The Time For Action is Now**

**Customers Want Data Protection**

**Shareholders Want a Healthy Organization**



# Questions



Ricky Link, CISA, CISSP, QSA  
14800 Landmark Blvd. Suite, 220  
Dallas, TX 75254  
Office 972-763-8011  
Ricky.Link@coalfire.com

