A Wake-Up Call?

*Fight Back Against Cybercrime*

Prepared for:

**ISACA North Texas Chapter**

Dallas Marriott Las Colinas
223 West Las Colinas Boulevard
Irving, Texas

October 8, 2015
Coalfire Background

- Leading Information Security Advisory Consulting Firm

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

- Sample Clients
  [List of logos for various industries including government, public sector, hosting/cloud service providers, service providers, utilities, retail, financial services, etc.]
Agenda

- Cyber Security Breaches are Nothing New
- A Wake Up Call For All Of Us!
- 2013 Retail Merchant Breach – An Example
- What is Needed – Defense in Depth
- Increased Government Oversight
- FISMA Annual Report to Congress Feb 2015
- Enough is Enough
- Questions
IBM estimates that over half a billion records of personally identifiable information (names, credit card information, social security numbers, etc.) were stolen in 2014.

77% of companies detected a security event in the past 12 months\(^{(1)}\).

Organizations on average detect 135 cybersecurity incidents each year\(^{(1)}\).

7% of U.S. organizations lost $1 million or more and 19% of organizations lost at least $50k in 2013 due to cybercrime incidents\(^{(1)}\).

84% of survey respondents believe the number of cyber attacks will increase\(^{(2)}\).

75% of survey respondents expect cloud security budgets to increase dramatically\(^{(3)}\).

The cybersecurity industry has experienced dramatic growth and levels of attention due to the recent increase in the frequency, size, and profile of cyber attacks.

---

(1) Source: PWC, Managing Cyber Risks in an Interconnected World, Sept. 30, 2014
(3) Source: IBM, 3rd Annual CISO Study, December 2014
High Visibility Incidents

Over the past 18 months, dozens of major cybersecurity breaches have been announced, collectively affecting hundreds of millions of people.
A Wake-Up Call – Cyber Risk is Nothing New

Coalfire Daily Media Report 5/28/2015

- Cybersecurity on the agenda for 80% of Corporate Boards
- Outlet: CSO
- Snippet: Cybersecurity is a topic of discussion at most board meetings, according to a new survey of 200 corporate directors.
A Wake-Up Call – Cyber Risk is Nothing New

Coalfire Daily Media Report 9/28/2015

- How Strong Are The Middle East’s Cybersecurity Networks?
- Outlet: Global Risk Insights
- Snippet: United Arab Emirates National Electronic Security Authority announced that cybersecurity is one of the biggest economic and national security challenges countries face in the 21st century. Studies show that hacks have been increasing over the last several years against major corporations in the Gulf, specifically where the majority of the region’s economic activity is situated.
A Wake-Up Call – Cyber Risk is Nothing New

Coalfire Daily Media Report 9/29/2015

- Raytheon Wins $1 Billion Cybersecurity Contract to Battle Attacks on U.S. Agencies
- Outlet: ABC News
- Snippet: The Depart of Homeland Security has awarded a $1 Billion cybersecurity contract Raytheon to shore up the federal government’s defenses against the increasing onslaught of attacks. The contract, one of the largest civilian cybersecurity orders in years, would help more than 100 federal civilian agencies protect their networks against malicious hackers, and it comes after the Office of Personnel Management suffered one of the most damaging breaches in history.
A Wake-Up Call – Cyber Risk is Nothing New

Coalfire Daily Media Report 10/6/2015 (24 Different Alerts)

- One Third of Companies Still Fall Short on Data Protection Policies By Misco.co.uk
- Watchdog: Cybersecurity Remains Top Challenge for Consumer Financial Protection Board & Fed By ABA Banking Journal
- Study Cites Cybercrime's Rising Costs to Corporations By Associated Press, CNBC
- Scottrade Acknowledges Two-Year-Old Data Breach By eSecurity Planet
- OIG Faults OCR Breach Investigations By HealthData Management
- Cyber Bill Likely to Hit the Senate Floor Soon By The Hill
- Into the Spotlight: Cyber Insurance By SC Magazine
- Hackers Breach Microsoft OWA Server, Steal 11,000 User Passwords By Softpedia
- NY AG Offers Guidance After Data Breach By Associated Press, Washington Post
- 7 Trump Hotels Hit by Data Breach By Associated Press, CBS News
- Nuclear Plants' Cybersecurity Is Bad -- And Hard to Fix By Dark Reading
- Krebs: Most Firms Fail to Take Simple Cybersecurity Measures By Forward Thinking
- More Data Breaches Caused By Lost Devices Than Malware or Hacking, Trend Micro Says By Network World
# Industry Trends & Drivers

## Trend

### Shift from Compliance to Risk Management

- Motivating force now to mitigate risk of cyber attack vs. simply complying with regulations
- Driven by large monetary losses, reputational damage, and potential litigation

### Increasing Reliance on Cloud & Technology

- Rapid expansion of big data, mobility, BYOD, and Internet of Things
- 86% of organizations moving to the cloud with 75% expecting cloud security budgets to increase dramatically\(^1\)

### 3rd Party Risk Management & Info Sharing

- Cyber criminals often find 3rd parties provide relatively easy access to systems
- e.g. Target’s HVAC vendor
- Increasing regulation (e.g., HIPAA Omnibus Rule)

### Continuous Diagnostics & Monitoring

- Point-in-time compliance checks no longer sufficient to manage risk
- Explosion of mobile/cloud results in companies’ environments changing dramatically on a daily basis

## Drivers

### Proposed Solutions

- Board level cyber risk advisory needed
- Validation of Technology & Cloud Service Providers
- Application Security Validation
- Sharing application that automatically populates end client security assessments with vendor’s information.
- Reduce need for clients to look upstream and downstream
- Architect with ability to incorporate best of breed security solutions
- Example: Security vulnerability scans today to automated penetration testing, threat detection, etc.

---

\(^1\) Source: IBM, 3rd Annual CISO Study, December 2014
The Blueprint for Attacks

All the recent security 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 NEEDED>>
Analysis of a 2013 Retail Merchant Breach

Advertisement for Stolen Credit Cards

Source: Krebsonsecurity.com

Source: Committee on Commerce, Science & Transportation
“A “Kill Chain” Analysis of the 2013 Data Breach” report dated 3/26/14
Analysis of a 2013 Retail 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
What is Needed? Defense in Depth

**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
What is Needed? 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
**What is Needed? Defense in Depth (iii)**

**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*
What is Needed? Defense in Depth (iv)

Cybersecurity Breach Response Plan: Internal response plan and external communications strategy while research, root cause analysis, consultation and technical support to investigate the origins of the breach. Utilize appropriate forensic tools to detect and respond to future incidents.

Prevented Steps: Propagation

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
Multiple Control Models and Regulations

- AICPA
- PCI Security Standards Council
- HIPAA
- CSA security alliance™
- FFIEC
- FedRAMP
- GLBA Compliance
- Texas Medical Privacy Act of 2012
- ISO-27001/2
- Privacy Laws
- SSAE 16 SOC 1/2

IT Security Controls:
- Training
- Security Policy
- Quality
- Security Arch. Design
- Code Review
- Penetration Testing
- NIDS/HIDS
- IDS
- Firewall
- Hosting
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...
Has Driven Increased Government Oversight

May 2014
Announced that it will conduct cybersecurity assessments to study the state of vulnerability and risk mitigation policies and preparedness across community banks

Encouraged public companies that are victims of cyber attacks to disclose additional information to help protect customers whose private data could be at risk

Formally launched CBEST, a new framework designed to help identify areas where the financial sector could be more vulnerable to sophisticated cyber attacks

Chairman Tom Wheeler urged the private sector to "step up to assume new responsibility and market accountability for managing cyber risks" while asking companies to report how they are adopting best practices and codes of conduct

Passed a bill to encourage greater sharing of information between the Federal government and the private sector, in part by protecting participants from lawsuits

Restructured its national security prosecution team to become better equipped to handle cyber attacks and created a new position in its senior ranks to focus on cybersecurity

Required all banks submit to quarterly penetration tests of their systems' vulnerabilities and may require obtaining R&Ws from 3rd party service providers regarding cybersecurity standards and policies in the future; also announced regular, targeted assessments of cybersecurity preparedness for all insurers following the Anthem breach

Created the Cyber Threat Intelligence Integration Center to coordinate cyber threat assessments and signed an Executive Order promoting hubs where companies can share cyber threat information with each other and the DHS; also launched sanctions program targeting international cyber attackers that threaten foreign policy, national security, or economic stability

Over the past 12 months, several Federal, State, and International Government Agencies have announced specific cybersecurity policies.
SEC – Disclosure Guidance

Disclose actual or suspected data breach

- Data breach with material impact
- “Management Discussion & Analysis” (See next slide)
- Financial Statement Impact

Disclose material risk of an incident – Risk Factors

- Inherent risk due to nature of the business environment ... to include outsourced functions
- Likelihood of past incident predicting future events
- Regulatory requirements and potential penalties
- Risk mitigation oversight
- Avoid ‘boiler plate’ descriptions of general risk factors that apply to all or most other registrants – SEC requires specific cyber issues. t insurance coverage
SEC – Management Discussion & Analysis

- **Business Description**
  - Inherent risk – material impact on clients, partners, industry
  - Competitive position
  - Viability of current or future products

- **Legal Proceedings**
  - Identification of ongoing or potential litigation with material impact
  - Description of impact or relief being requested

- **Financial Statement Disclosure**
  - Remediation, investigation and recovery costs
  - Security program enhancements
  - Litigation costs and fines
  - Reputation damage or impairment of future earnings

- **Disclosure Controls and Procedures**
  - Impact on future reporting for the registrant
Annual Report to Congress:

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.

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
Where is Our Data Coming From Now?  
...The Internet of Things (IoT)
Orgs Tend to Over-Estimate Their Compliance

- Unnecessary vulnerable services not removed
- Inadequate access controls and vulnerable remote access
- Default system settings and passwords
- Missing or outdated security patches
- Policies & procedures incomplete
- Inadequate or no firewall
- Missing or outdated Anti-virus Anti-malware software
- Improper Implementation
- Poorly coded web applications
- Lack of monitoring
- Lack of network segmentation
- Lack of logging
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 your critical systems
    - 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, CISM, QSA, CGEIT  
Dallas, TX  
Office 972-763-8011  
Ricky.Link@coalfire.com