Communicating About Cybersecurity in the Board Room
Q1 2016
Agenda

Welcome & Introductions
Breakfast Discussion
Panel Discussion & QA
Best Practices
Wrap Up
Current Events

Target CEO Fired - Can You Be Fired If Your Company Is Hacked?

A common perspective is that cyber security is primarily the responsibility of the IT department. If a data breach incident occurred, the senior IT executive was the only one to take the fall, and usually only if there was incompetence involved vs. simply bad luck.

Forbes

Obama Wants $19 Billion To Fix Federal Government Cybersecurity Failures

Thomas Fox-Brewster, Forbes Staff

The Market Isn't Buying That Deutsche Bank Is 'Rock Solid'

Frances Coppola, Contributor

CEO heads may roll for security breaches in wake of Sony boss’ exit, experts say

Feb 9, 2015, 8:54am PST - Updated Feb 11, 2015, 10:28am PST

INDUSTRY NEWS - TECHNOLOGY
Nearly 90% of all organizations report at least one insider threat each month.

76% of all organizations reported at least 1 compromised account each month.

2015 Sandhill Security Study
Impact of Current Events

- Cybersecurity is a Board Room Topic
- No C Level is Safe
- The Attacks and Risks are Compounding
Perception

C-suite view of the probability of a significant breach

94% give it some probability > 0%

 Believe there's no chance it will happened to them

 6%

 Believe the odds are MORE than 50%

 14%

 Believe the odds are LESS than 50%

 80%

Source: IBM Institute for Business Value.

Denial...not just a river in Egypt
Perception

Strength of cybersecurity plans by role

% C-suite respondents that report the cybersecurity strategy of their enterprise is well established

- CRO: 77%
- CIO/CTO: 76%
- COO: 70%
- CSCO: 66%
- CLO: 63%
- CHRO: 61%
- CMO: 59%
- CFO: 55%
- CEO: 51%

Source: IBM Institute for Business Value.
Almost half of Boards still view cybersecurity as an IT matter, rather than an enterprise-wide risk issue.

- pwc 2015 Cybercrime Survey
BoD, C Level Perception

- We bought product / solution “x”.... We are secure
- We just spent $_____ ...why are we not “secure”
- We just hired ____ ....how come we need more people?
- Vendors have (some or all) of the answer to security
- CISO/CIO need to own the problem
- CISO/CIO have been empowered to “fix” the problem
- Do we “really” need to be compliant?
- A colleague told me they found a “work around” to compliance...what’s the “work around”?
Realities

Lack of Executive Leadership Team Respect

• July 2015:
  – 44% believe CISOs should be accountable for any organizational data breaches
  – 54% believe CISOs should not be responsible for cybersecurity purchasing decisions

• Chief Scapegoat Officer anyone?
  – 61% do not believe their CISO would be successful in a leadership role outside of security
  – 51% believe it was “unfair” for the Target CEO and CIO to be fired in the wake of its data breach...

CISO, CIO Perception

- We don’t “own” the problem – we are not “empowered”
- BoD, C Suite is too high level
- They “don’t get it” or They “don’t want to “get it”
- They have unrealistic expectations
- We lack the $, time and resources to drive change
Realities

65% of C-suite executives are very confident their cybersecurity plans are well established, yet only 17 percent demonstrate the highest levels of preparedness and capability.

68% of CEOs are reluctant to share security incidents externally, yet external collaboration is recognized as a powerful offensive capability against cyber-criminals.

60% The CFO, CHRO and CMO feel the least engaged in cybersecurity threat management activities, yet are the stewards of data most coveted by cybercriminals.

Lack of Alignment with CISO/CIO
80% of CISOs say the challenge posed by external threats has increased in the last three years (42 percent said dramatically).

59% of CISOs strongly agree the sophistication of attackers is outpacing the sophistication of their organization’s defenses.

40% of CISOs report that sophisticated external threats are their top challenge.

Increasing Threat Sophistication Outpacing Organization Response Capabilities
Lack of Security Maturity Compounding Issues and Risks
The Chasm: Perception is Reality

- If you were empowered could you drive changes within internal team, departmental, organizational behavior?
- If you had the $ and resources, could you fix the problem?
- If you had the charter of increasing awareness and driving education, how would you do it?

- Do you really want to “own” the problem?
- What is the “real” problem?
Crossing the Chasm

- We Need to Own the Conversation
  - Awareness & Education
  - Accountability & Authority
  - Levels of Responsibility
  - Communication & Escalation
Panel Discussion

- Danger Zone Items/Topics/Approaches
- How to Realize ROI from Tech Investments
- Playing Offense

CISO Playbook: Suit-up & Play Offense

In the game of IT security there are thousands of tools available, but the very best strategy to prepare for an opponent is to know your own weaknesses.

"Some of us will do our jobs well and some will not, but we will all be judged on one thing: the result." – Vince Lombardi
Examples of What is Working

- Approach Examples
- Communication Methods
- Presentation of Data (Current State) Examples
- Recommendations Examples
GRC Approach Example

- Step One: Draw the Big Picture
- Step Two: Demonstrate Specific Impact
- Step Three: Get into the Details
- Step Four: Find the Right Metaphor
- Step Five: Create the Delivery Methods

Source: Carole Switzer, President OCEG
Future State Example

**Current State**
- Managed in silo's
- Reactive
- Project or program approach
- Separate from mainstream processes and decision-making
- Necessary evil
- Fragmented use of technology

**Future State**
- Enterprise approach
- Proactive
- Systemic approach
- Embedded within mainstream processes and decision-making
- Value-added
- Architected solutions

© 2013 OCEG
Using 3rd Party Research

US cybersecurity: Progress stalled
Key findings from the 2015 US State of Cybercrime Survey

7 reasons why cybersecurity is a Board oversight issue
Cyberthreats are among the most significant business risks facing organizations today—and Boards are now held accountable. As a result, directors must view cybersecurity as an enterprise-wide risk issue that should be addressed from strategic, cross-functional, and economic perspectives. Following are seven reasons why Boards should be asking serious questions about cyberthreats and their organization’s cybersecurity capabilities:

1. The impact of cybersecurity is systemic. Incidents can impact an organization’s global operations even when a risk point is thousands of miles away.
2. The financial impact can be significant and can include costly class-action lawsuits, which may reflect on Boards’ fiduciary responsibility to preserve corporate financial value.
3. As regulations evolve, compliance is becoming more challenging and increasingly costly. The European Union’s Data Protection Directive, for instance, includes a proposal for fines of up to 5% of a company’s global revenue. This also lays the foundation for civil litigation.
4. The Internet of Things has brought new threats, including compromise of industrial controls and smart building systems that can cause extreme risks and tremendous physical damage.
5. Cybersecurity insurance should be considered as a regulatory hedge against cyber-risks. A risk committee should ask questions regarding coverage for directors’ and officers’ liability, commercial general liability, prior acts, and property and casualty insurance.
6. Adversaries such as nation-states and organized crime are working together to attack organizations for objectives like economic sabotage, theft of trade secrets, money laundering, terrorism, and military and intelligence operations.
7. Cyberattacks can result in substantial financial losses and damage brand reputation by disrupting an organization’s strategic objectives, such as a planned merger or acquisition, the launch of a new product, or a business deal with a potential customer.

---

Communication Methods

- Text or Video?
- Bullets or Graphics?
- Paragraphs or Sentences?
- Reports or Executive Briefings?
- Internal Review or Third Party Validation?
Private Equity Example

- Engagement Objectives (Business, Financial, Risk Drivers)
- Market Trends (IoT, Threats-Attacks, Regulation, Big Data)
- Myths (Too Insignificant or too Small to Hack, Security is a IT Issue)
- Key Themes (Change is Difficult, Being Secure, No Silver Bullet)
- IT Collateral Findings (Employee day to day issues-feedback)
- Findings (Key Metrics, Controls, Vulnerabilities, Impact to Business)
- Recommendations
- Roadmap
- QA
Findings Portfolio Overview: Key Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unencrypted Sensitive Data</td>
<td>Yes</td>
</tr>
<tr>
<td>Facility Security Infrastructure Controls In Place</td>
<td>61%</td>
</tr>
<tr>
<td>Top external risk</td>
<td></td>
</tr>
<tr>
<td>Web Servers</td>
<td></td>
</tr>
<tr>
<td>Top internal risk</td>
<td></td>
</tr>
<tr>
<td>Patching</td>
<td></td>
</tr>
<tr>
<td>Phishing attack success</td>
<td>24%</td>
</tr>
<tr>
<td>Hosts</td>
<td>1,223</td>
</tr>
<tr>
<td>Avg vulnerabilities per host</td>
<td>185</td>
</tr>
<tr>
<td>Avg # Critical Vulnerabilities</td>
<td>7</td>
</tr>
<tr>
<td>Avg # High Vulnerabilities</td>
<td>40</td>
</tr>
<tr>
<td>Avg # Medium Vulnerabilities</td>
<td>126</td>
</tr>
<tr>
<td>Avg # Low Vulnerabilities</td>
<td>12</td>
</tr>
<tr>
<td>Sensitive Data Discovery</td>
<td></td>
</tr>
<tr>
<td>Unencrypted Credit</td>
<td>1,703</td>
</tr>
<tr>
<td>SSN</td>
<td>232,215</td>
</tr>
<tr>
<td>Driver’s License</td>
<td>1</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>46</td>
</tr>
</tbody>
</table>
Findings

Security Control Assessment

Security Controls Implementation

- Controls Implemented 35% (n=33)
- Controls Not Implemented 33% (n=31)
- Controls Partially Implemented 29% (n=28)
- N/A 3% (n=3)
Findings

Security Control Assessment

Security Controls Risks

High

11 / 19%

Medium

36 / 63%

Low

10 / 18%
Findings

Security Control Assessment Implementation degree by area

- Technical: 50%
- Administrative: 70%
- Physical: 80%

Opportunity for improvement

Goal: 85% implementation
Findings Impact to Business

• Increased costs from inconsistent processes

• Compliance impact from lack of documentation

• Social engineering / theft / corporate espionage
Findings

Vulnerability Cloud

Insecure-Windows-Service
Google Software
Antivirus
Code-Management
FLEXnet-Connect-Updates
HP Printer firmware
Apache
CGI
Virtualization
OracleRDBMS
Open-Source-Software
MS-Patches
Java
PHP Code
Microsoft OS
OpenSSL
VMWare
HP Software
Encryption
Adobe-Patches
Apple Software
Heartbleed
BEAST
Linux
ShellShock
Novell
WindowsServicePack
Poodle
SAP-OS
HP-Version Control
Unsupported Web Server
3rd Party Software

Copyright 2016 © Terra Verde, LLC.
All rights reserved.
Findings External Network Vulnerabilities

- Low: 42
- Medium: 555
- High: 124
- Critical: 20
### Findings Internal Network Vulnerabilities

<table>
<thead>
<tr>
<th>Level</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>1,941</td>
</tr>
<tr>
<td>Medium</td>
<td>11,365</td>
</tr>
<tr>
<td>High</td>
<td>13,333</td>
</tr>
<tr>
<td>Critical</td>
<td>2,176</td>
</tr>
</tbody>
</table>
Findings Patch Analysis


Values: 54, 1,443, 1,990, 840, 529, 2,170, 2,872, 3,339, 9,321
Findings  Impact to Business

• Lack of process = easier target

• Exploits for older vulnerabilities are automated which makes likelihood of exposure easier, by less technically adept attackers.

• Social engineering exercise demonstrated that there is a reasonable possibility for users to click on malicious emails that could lead to exploitation.
Key Metrics Portfolio Overview

Physical Security

Security Program / Controls

Social Engineering

Vulnerability Management Program

Sensitive Data Discovery

1 No Threat
2 Low Threat
3 Medium Threat
4 High Threat
5 Critical Threat
Recommendations

1. Change is difficult
   - Establish security as a cornerstone of your cultural fabric
     - Messages with the right lever move mountains
   - Implement appropriate governance and other key processes
     - PE Firm should consider developing and communicating portfolio policies
     - Initiate a documentation effort within IT to ensure ad hoc processes are written down
   - End-of-support / end-of-life systems should be replaced
     - Compliance and security risks if refresh is not occurring on a routine basis
   - Determine efficiency of intra-portfolio opportunities
     - Establish intra-portfolio teams to discuss best practices & collective purchasing
Recommendations Implementation Timeline

- **People**
  - Hiring dedicated security staff
  - Increase awareness and Training

- **Process**
  - Governance Processes (Vuln/Patch/Change Mgmt)
  - Reporting

- **Technology**
  - Patch vulnerabilities
  - Monitoring

Timeline:
- 0-1 month
- 3 months
- 6 months
- 9 months
- 1 year
Best Practices Summary

- Think About Establishing Proactive Teams
- Usage of Frameworks
- Standards Can Help Unify Scales
- Multiple Measurements
- Understand Impact of Cloud & IoT
- Build a Risk Culture
Collaborate, Educate, Empower: IBM

- **Establish a security governance model and program** to encourage enterprise-wide collaboration
- **Empower the CISO** with the mission of managing information security risk across the enterprise, as well as lead the initiative among the C-suite
- **Elevate and regularly discuss cybersecurity at C-suite** and board meeting agendas and engage Risk, Finance, Marketing, Human Resources and Supply Chain at a minimum
- **Drive executive level education**
- **Include the C-suite** in developing an incident response plan and share it with the board
Resources

- Real World Approach
- 3rd Party Research
- Visuals
- Support Groups
Wrap Up

Risks and attacks will increase
We need to drive awareness, education
Drive the accountability conversation
Be responsible for the solution
Appendix
Corporate Highlights

FAST FACTS

- Founded in 2008 by Cyber Security, Risk, Compliance Executives & Experts
- Headquartered in Phoenix Arizona (40 FTEs)
- Security, Risk, Compliance Consulting
- One of the Largest PCI QSA in Arizona
- Hundreds of Engagements Performed Across Multiple Continents Annually
- Invested Millions of Dollars, Thousands of Hours Developing TruSOC™ - Managed Security Service
- TruSOC™ utilized by customers across the U.S.
- Ongoing Investments in Services Portfolio, Technologies, Sales & Distribution Channels
Customers by Industry
Credentials
Technology Partners

- Vensys
- Sophos
- Fortinet
- Tenable
- Imperva
- Survela
- RedSeal
- Incapsula
- Airtight
- Amazon Web Services

Copyright 2016 © Terra Verde, LLC. All rights reserved.
Industry & Association Involvement

RSA Conference
ISACA
DEFCON
ISSA
PCI Security Standards Council
TRIBALNet
ASU West
Arizona Technology Council
Northern Arizona University
Arizona Eller Cybersecurity Forum
CSA Security Alliance
Growing Market

Figure 8: Cybersecurity spending in the U.S., percent of GDP and USD billions, 2009-2017

Cyber-risk spending priorities

47% New technologies
40% Audits & assessments
33% New skills & capabilities
24% Redesign cybersecurity strategy
15% Redesign processes
15% Participate in knowledge sharing

pwc 2015 US State of Cybercrime Survey
Maturity Model Stages

**REACTIONARY**
- Firewall and Antivirus
- No Full Time Management
- No Strategy or Standards

**INFORMAL**
- Firewall and Antivirus
- Tech Buying (Spot Solutions)
- Finance Oversight
- Compliance Focus
- Adhoc Policies

**REPEATABLE**
- Firewall and Antivirus
- IPS/IDS
- Tech Heavy/Patching
- SDLC
- Minimal Controls/Policies
- Stop Gap Dedicated Management
- Compliance Focus
- Tribal Knowledge
- Some Practices

**DEFINED**
- Technology Overhaul/Standards
- Documentation Controls
- Policies
- More than 1 Person in Team
- Training & Education
- Outside of IT

**MANAGED**
- Level 3+
- Governance Maturity
- Security Process Automation
- System Integration
- Expansion of Team

**OPTIMIZED**
- Level 4+
- Security Integrated Across Business
- Top Level Program
- with Best Practices
- Security = Core Corp Value
Consulting Services

ASSESSMENT & TESTING
- Penetration Testing (Internal & External)
- Web Application Penetration Testing
- Wireless Penetration Testing
- Code Review
- Physical Penetration Testing
- Advanced Persistent Threat
- Internal & External Server Side Attacks
- Client Side Attacks
- Vulnerability Scanning
- Security Assessments
- Risk Assessment
- Social Engineering
- Phishing

AUDIT & COMPLIANCE
- PCI DSS Readiness
- PCI DSS ROC
- PCI Toolkit
- HIPAA Security Rules Assessment
- ISO 27001/2 Security Assessment
- IT Audits
- FTC Audit
- NIST Audit & Assessment
- Compliance Gap Analysis
- Compliance Program Development & Tracking

SECURITY STRATEGY
- Strategic Planning, Metrics, Budgets
- Policy & Procedure Development
- Business Continuity Planning Analysis
- Disaster Recover Planning Analysis

BUSINESS & RISK
- Risk Program, Tech, Project Assessment
- Incident Response & Digital Forensics
- Litigation Support
- Vendor Review & Assessment
- Subject Matter Expert Advisory
- Security Education & Awareness Training

TECHNOLOGY INTEGRATION & TRAINING
- Alien Vault Training
- Alien Vault, Sophos, Fortinet, Imperva, Incapsula, Fortinet, Palo Alto, Cisco Tenable Installation
Managed Solutions

TRUSOC
- Vulnerability Assessment
- Asset Discovery
- Threat Detection (Host & Network)
- Behavioral Monitoring (Log, Packet, Avail)
- Security Intelligence (SEIM Cor, Feeds)
- Security Operations (Logs Reviews)
- Security Operations (SLA)
- Security Operations (Monitoring)
- Security Operations (Continuous Improv)
- Security Operations (Directive Updates)
- Security Operations (Reporting, Com)
- Security Operations (Platform Maint)

MANAGED PHISHING
- Phishing Program Design
- Phishing Pilot / Assessment
- Phishing Simulation Templates
- Phishing Campaign Management
- Reporting & Monitoring
- Education & Awareness Training
- Compliance Tracking

VENDOR RISK ASSESSMENT
- Customized Assessments & Screening
- Customized Workflow & Analysis
- Assessment Portal & Platform
- Vendor Assessment Online
- Vendor Assessment Onsite (if needed)
- Inspection, Research, Validation
- Dashboard, Customized Reporting

SETA TRAINING & LMS
- Customized Security Education Training and Awareness (SETA) Modules
- Learning Management System (LMS)
- LMS Integration and Management
Ed Vasko
CEO
Cell: +1 692-758-3491
Office: +1 877-707-7997, x4
Ed.vasko@tvrms.com

Carlos Villalba
VP Solutions
Cell: +1 315-491-1320
Carlos.villalba@tvrms.com