Risky Business
Is Your Cybersecurity in Cruise Control?
Midland Oil & Gas CPE
January 14, 2016

What We’ll Cover

• About me
• Background
• The threat
• Risks to your organization
• What your organization can/should be doing
• The role of audit
• About Weaver

About Me

Brittany George, CISA, QSA
Weaver
Senior Manager
IT Advisory Services

• Provides security, SOC, IT Audit (GRC), security and process improvement consulting services
• More than 11 years experience in IT auditing, security, and consulting
  (TXU/Capgemini Energy, KPMG, Weaver)
• BBA in MIS from the University of Oklahoma – Boomer Sooner!
• Board member, ISACA North Texas
• Steering committee member, Cloud Computing and Cyber Forums of Tech Titans

Disclaimer

• The comments and statements in this presentation are the opinions of the speakers and do not necessarily reflect the opinions or positions of Weaver and Tidwell, LLP.
• This presentation is the property of Weaver and Tidwell, LLP. All rights reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form without written permission from Weaver and Tidwell, LLP.
• Weaver and Tidwell, LLP expressly disclaims any liability in connection with the use of this presentation or its contents by any third party.
“Some organizations will be a target regardless of what they do, but most become a target because of what they do. ...”

If your organization is indeed a target of choice, understand as much as you can about what your opponent is likely to do and how far they are willing to go.”

-2013 DBIR, pg. 48

Background

In 2015, there are two kinds of companies:

1. those that have been breached
2. those that know they’ve been breached

Who are the victims of breaches?

- Financial organizations
- Public sector
- Technology/Information
- Retail and restaurants
- Manufacturing, transportation, utilities
- Professional services firms
Who are the bad guys?
Depends on what information assets or systems you have.
Could be:
- Nation states like China, Russia, Iran, North Korea
- Hacktivists (Anonymous, Wikileaks)
- Terrorist organizations
- Organized crime
- [http://map.ipviking.com/](http://map.ipviking.com/)

What do they want?
Depends on what information assets or systems you have.
Could be:
- Defense secrets
- Disruption of critical infrastructure
- Trade secrets and intellectual property
- Confidential information about your organization, your business dealings, or your customers
- Exploitable consumer financial information

How do breaches occur?
- 45% trusted insider
- 44% malware
- 27% some form of hacking
- 26% SQL injection
- 24% password compromise
- 19% targeted attack
- 12% lost, stolen, hijacked device
- 5% other

What are the commonalities?
- Financial motives
- Targeted user devices
- Compromised servers
- Opportunistic attacks
- Discovery by external parties
- Time of discovery is multiple months
- Low difficulty of initial intrusion
Risk to Organizations

**Key risks to cyber theft:**
- Liability for loss of confidential information, loss of private consumer information, business interruption, or even loss of human life
- Loss of intellectual property / trade secrets / competitive advantage
- Damage from loss of confidentiality
- Reputational damage

Risk Impact

Gone are the days we could bury our heads in the sand

- Liability is increasing:
  - Target
  - Yahoo
  - CF Disclosure Guidance: Topic No. 2 – Cyber Security

Becoming a Target
Becoming a Target

- 40 Million credit / debit cards
- 46% Drop in profit 4Q 2013
- $200 million lost by banks reissuing cards
- $100 million planned by Target to upgrade to Chip and Pin cards
- 1 HVAC Vendor with network access
  - Gained access to the system by using stolen credentials from a third-party vendor.
  - A refrigeration and heating company near Pittsburgh whose data connection to Target was purely for billing, contract submission, and project management.

Would your risk management program identify this vendor as high risk?

What do we do?

“Prevention is ideal, detection is a must!”
What to Do

Organizations should:

• Classify data
• Implement an ISMS
• Implement tools to identify security events
• Perform periodic security assessments based on the specific threats
• Consider cyber counterintelligence

Risk Identification

It begins with...

Risk Identification seeks to identify and address risks... instead of after they have impacted the company of reacting to risk events...

Stage 1 - Root Cause Event Signal

• Factors/signals are present that create a high risk environment.
• Can be identified through monitoring of Key Risk Indicators

Stage 2 - High Risk Environment

• A high risk environment has resulted from the signals identified in Stage 1.
• High potential for root cause event.

Stage 3 - Root Cause Event

• An event occurs that creates potential for significant risks to be realized.

Stage 4 - Risk Realization and Consequence

• A significant risk event occurs, impacting the company.
• A snowball effect can occur, causing risks to multiply at this stage:
  - Reputation risk
  - Fraud risk

Stage 5 - Management/Mitigation

• Management evaluates outcome and establishes mitigation strategy to avoid future risk.
Lifecycle of a Risk Event

Stage 1 - Root Cause Event Signal
- Tire pressure is low

Stage 2 - High Risk Environment
- Flat tire

Stage 3 - Root Cause Event
- Car Accident

Stage 4 - Risk Realization and Consequence
- Increased insurance cost
- Relegated to high risk pool
- Inability to negotiate terms
- Switch insurance providers
- Wait for accident to clear from record
- Take defensive driving
- Check tire pressure regularly

Stage 5 - Management / Mitigation
- Switch insurance providers
- Wait for accident to clear from record
- Take defensive driving
- Check tire pressure regularly

If the risk had been identified here through monitoring of Key Risk Indicators...

... the cause event may never have occurred...

... and the risk may never have been realized.
The biggest challenge is **getting the data!**

You may have to create a process to obtain it.

---

**Risk Definitions**

**Risk Assessment** is NOT the same as **Risk Management**.

**IDENTIFY & EVALUATE**

**Risk Assessment:**
The process of identifying and evaluating individual risks for the purpose of determining risk responses.

**Respond & Manage**

**Risk Management:**
The process of identifying, assessing and responding to risk on an ongoing basis. Requires building the processes to manage the risk.
Risk Assessment - How

1. Build a high-level risk profile for existing third parties, departments, functions and rate it.
2. Establish risk factors and evaluate each against relevant risk factors.
   For example, customized to your environment:
   - Financial
   - Regulatory
   - Operational
   - Reputation
3. Do further investigations based on risk assessment.
4. Establish a more detailed risk assessment based on investigations, not only a rating but a description of the potential risks.

Evaluating Cyber Risk

- The process of identifying risk upfront (for example, WHILE you evaluate third parties).
- Build a program, periodic risk identification considerations.
- Example of risk identification program: Vendor profiling.
  - Financial stability
  - Control environment
  - Technology environment
  - Dependency
  - Access to information / intellectual property
  - Critical in supply chain
  - Regional risk
  - Operational characteristics
  - Regulatory / compliance interaction

Other Types of Risk

- Global cybersecurity skill shortage + increased budgets = Career Opportunities
- The idea professional
  - 33% need training and/or certified
  - 43% need more information
  - 33% need to protect
  - 40% need to protect
  - 69% need more information
  - 69% need more information

Risk Response
Develop Risk Responses

When developing responses, management considers four alternative responses:

- **REDUCE**
  - Implement mitigating controls

- **ACCEPT**
  - Take no positive action to mitigate the risk

- **AVOID**
  - Stop engaging in any activity that creates the risk

- **SHARE**
  - Share the risk with a third party, e.g., insurance policies

As a part of this process, management:

- Evaluates costs/benefits of available risk responses
- Analyzes whether risk responses appropriately reduce risk to tolerable level
- Selects most appropriate risk response based on risk appetite, risk tolerance, and evaluation of portfolio risk

Standards and Names

**Trust Services Principles and Criteria**

- **Services Org Control 1 (SOC 1)**
  - SSAE16 - Service auditor guidance
  - Restricted Use Report (Type I or II report)
  - Purpose: Report on controls for F/S audits

- **Service Org Control 2 (SOC 2)**
  - AT 101
  - Generally a Restricted Use Report (Type I or II report)
  - Purpose: Report on controls related to compliance or operations

- **Service Org Control 3 (SOC 3)**
  - AT 101
  - General Use Report
  - Purpose: Report on controls related to compliance or operations

Common Third Party Assurance

- What is the specific scope of each?
- What are the areas of overlap?
- What are the unique areas for each audit type?
- What are some other third party IT audits?

Common Third Party Assurance

**SOC 1**

ISO 27001

**SOC 2 & 3**

**PCI DSS**

SOC 1 SM Report

Report on controls at a service organization relevant to a user entity’s internal control over financial reporting

Contents of report package:

- Description of service organization’s system
- CPA’s opinion on fairness of description, suitability of design, operating effectiveness of controls
SOC 2SM Report

Restricted Report

Service Org Control 2 (SOC 2)

AT101

Generally a Restricted Use Report (Type I or II report)

PURPOSE: Reports on controls related to compliance operations

Example:
A Software-as-a-Service (SaaS) or Cloud Service Organization that offers virtualized computing environments or services for user entities and wishes to assure its customers that the service organization maintains the confidentiality of its customers’ information in a secure manner and that the information will be available when it is needed.

SOC 3SM Report

General Use

Service Org Control 3 (SOC 3)

AT101

General Use Report

PURPOSE: Reports on controls related to compliance operations

Trust Services Report for Service Organizations

Contents of report package:
- CPA’s opinion on whether entity maintained effective controls over its system

SOC 2SM Report

5 Trust Services Principles

Security (Common Criteria)
The system is protected against unauthorized access (both physical and logical)

Availability
The system is available for operation and use as committed or agreed

Processing integrity
System processing is complete, accurate, timely and authorized

Confidentiality
Information designated as confidential is protected as committed or agreed

Privacy
Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity’s privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants

What’s the difference between Type 1 and Type 2?

Both report on the fairness of the presentation of management’s description of the service organization’s system, and...

Type 1
- Reports on the suitability of the design of the controls to achieve the related control objectives included in the description
- As of a specified date (i.e., as of June 30, 2013)

Type 2
- Also reports on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description
- Throughout a specified period (6 to 12 months)
Relying on an Audit

Key Considerations

- Confirm the type of report, its purpose and its scope
- Evaluate the coverage within the report in relation to the areas of concern based on risk
- Have the right personnel evaluate the reports
- Push back and insist on performing your own audit (when necessary)
- Validate the external audit firm

The ultimate risk response is an ongoing program that identifies, assesses and responds to cyber risk

- Data classification and protection
- Preventative and detective measures
- Evaluating and monitoring partner relationships

Cyber Risk Considerations

Key Focus Areas

- Intelligence-driven security and risk management
  
  Proactive versus Reactive

  Intelligence collections that enhance audit
  
  Are policies and controls effective?

  Validate internal threat and risk assessments
  
  Are our perceived threats real and did we prioritize them correctly?

About Weaver
About Weaver

Weaver is a leading accounting firm in the Southwest with offices in Fort Worth since 1950. We have over 550 employees from 21 countries, including China, France, Serbia, Zimbabwe, and many more.

IT Advisory Services

At a Glance

- Resource Optimization
  - Software Selection
  - IV&V
  - General Controls
  - Application Controls

- Security & Availability
  - Information Security
  - Data Privacy
  - Business Continuity/Disaster Recovery

- Risk Management
  - IT Risk Assessment
  - IT Audit
  - Project Risk Management
  - Service Organization Control

- Compliance
  - Payment Card Industry (PCI)
  - Gramm-Leach-Bliley
  - Sarbanes-Oxley
  - HIPAA
  - FFIEC & FDICIA

Discussion

Brittany George, CISA, QSA
Senior Manager, IT Advisory Services
Tel: 972.448.9299
Brittany.George@Weaver.com