Institute of Internal Auditors

UT Dallas Fraud Conference – March 23, 2018

CYBER SECURITY AND FRAUD

CYBER SECURITY AND FRAUD

Cyber Security is everybody's business

- Management
- Staff
- Customers
- Public
- IT Department
- Internal Audit

CYBER SECURITY AND FRAUD

Cyber Security is all about risks:

- How much do we spend?
- Do we make intelligent decisions?
- Do we understand technology?
- Does Technology have risks?

Internal Audit's role is to help management understand these risks

CYBER SECURITY AND FRAUD

Consequences of a Cyber Attack

- Hit to your reputation
- Lost customers
- Diminished credibility
- Cost of repairing the damage

Companies will do everything they can to defend against cyber attacks

CYBER SECURITY AND FRAUD

Normal reactions to a Cyber Attack

- Companies tend to be reactive.
- They throw money at every weakness they discover.
- Fail to consider the bigger picture.
- Spend limited resources where they feel will do the most good.

CYBER SECURITY AND FRAUD

Major considerations for a proper defense:

- Companies don't have unlimited resources to defend against all cyber attacks.
- The potential impact on business if you had a breach.
- How would it affect business?
- How would it affect the achievement of their objectives and their successes?
- How much it is going to cost?

CYBER SECURITY AND FRAUD

What we need is better detection of Cyber Attacks

- Need to understand the impact on business.
- How it would affect the achievement of your objectives?
- How much is it worth spending to protect your assets?
- Place priority on understanding when & how you get breached?
- How to react to the breach?

CYBER SECURITY AND FRAUD

Internal Audit has an important role to play in managing cyber-risks.

- Help management navigate the breaches.
- The average breach takes 9-12 months to detect.
- Provide objective information to management to help them understand risks in terms of business.
- Bridge the business side & technology side.

CYBER SECURITY AND FRAUD

City of El Paso Cyber Attack Case Study

- $95 Million Street Car Project
- Managed by a Regional Mobility Authority (RMA)
- City of El Paso is the Fiscal Agent
- Invoices paid by the City on behalf of the RMA
- 2 Separate incidents, $300,000 & $2.9 million payments.
- Fictitious email traffic by an imposter.

CYBER SECURITY AND FRAUD

City of El Paso Cyber Attack Case Study

- Penetrated our Vendor Management System.
- Changed vendor ACH banking information.
- Redirected 5 vendor payments.
- When discovered, ACH recalls were processed.
- Partial recovery of ACH Vendor payments
- Local Police and FBI were contacted.

CYBER SECURITY AND FRAUD

City of El Paso Cyber Attack Case Study

- Internal Controls detected breach two times.
- Management overrode the detections twice.
- ACH Recalls recovered part of the payments.
- Time is of the essence in recovery efforts.
- Cooperation among organizations is the key to prevention and detection.

CYBER SECURITY AND FRAUD

Route Fifty Special Report published October 2016. Interview with Virginia Governor Terry McAuliffe, chair of 2016-17 National Governors Association Executive Committee

Survey of State Chief Information Security Officers in state government found that 60% of reported Cyber issues were discussed quarterly with state leadership.

How about your organization?

CYBER SECURITY AND FRAUD

- 30% of CISOs surveyed now report to their respective state's governors monthly on Cyber issues.
- 80% of CISOs state that lack of funding to handle Cyber Security threats remain a top concern.
- Having an established information security strategy can lead directly to more resources, both in funding and staffing.

CYBER SECURITY AND FRAUD

State of Virginia since Jan. 2016 to October 2016

- 53 million Cyber Attacks
- 1 every 4 seconds
- 300,000 per day
- Data contains Health Care & State Tax info
- Adopted National Institute of Standards & Technology (NIST) Framework
- Adopted advanced credit card standard. Using new chip technology for credit cards

CYBER SECURITY AND FRAUD

Major Challenges:

- State & local governments often lack the resources of their federal counterparts in investing in Cyber Security.
- The Federal Government has a hard time recruiting Cyber Warriors because they can go into the private sector and earn 3-4 times more money.
- Cyber Security has a huge economic impact in the State of Virginia. 67,850 people are employed & over 17,000 open jobs with starting pay of $88,000 in the Cyber Security profession.

CYBER SECURITY AND FRAUD

Penetration Testing Project

- Researched the Texas Directorate of information Resources for a Penetration Testing Vendor.
- Requested a Request for Qualifications from 3 vendors. Only 1 vendor responded.
- Established a Statement of Work for vendor to follow.
- Requested a quote.

CYBER SECURITY AND FRAUD

Penetration Testing consists:

1. Phase I – Discovery
2. Phase II – External Vulnerability Assessment & Penetration Test
3. Phase III – Internal Vulnerability Assessment & Penetration Test
4. Phase IV – Application Vulnerability & Penetration Test
5. Phase V – Wireless Penetration Test
6. Phase VI – Social Engineering Test
7. Phase VII – Presentation of Findings & Closeout
8. Extra Phase – Cyber Security Management Program Assessment

CYBER SECURITY AND FRAUD

Phase I - Discovery

- Review of the IT environment for Penetration Test.
- Review Network design
- Establish meetings cycle with Project Team.

Phase II – External Vulnerability Assessment & Penetration Test

- Scan firewalls
- Review potential external vulnerabilities
- Attack the firewalls and servers

CYBER SECURITY AND FRAUD

Phase III – Internal Vulnerability Assessment & Penetration Test

- Attack routers by use of passwords.
- Assess network configuration
- Review network monitoring activities to detect intruders

Phase IV – Application Vulnerability Assessment & Penetration Test

- Perform penetration testing on financial applications
- Test financial applications for authentication, authorization, and auditing.
- Test data protection in transit and at rest

CYBER SECURITY AND FRAUD

Phase V – Wireless Penetration Test

- Review potential vulnerabilities on Wireless network
- Wireless Penetration Test
- Test authentication method & encryption

Phase VI Social Engineering Test

- Email phishing attacks
- Phone calls
- Test physical security controls

CYBER SECURITY AND FRAUD

Phase VII – Presentation of Findings & Project Closeout

- Final Project Meeting to review findings
- Acknowledge Project Completion
- Issue Final Report

CYBER SECURITY AND FRAUD

Phase VIII – Cyber Security Management Program Assessment

- Review IT Security Policies
- Review IT Organizational Structure
- Review skills & certifications of IT, Help Desk, Security staff, application developers
- Review Network infrastructure & equipment
- Internet access
- Phone & email system
- Wireless LAN
- Remote Access Controls
- Public Websites

CYBER SECURITY AND FRAUD

Conclusion

If you don't work on Cyber Security on the front end, you will pay for it on the back end. What you will pay for on the back end is a number that can't be measured or estimated.

CYBER SECURITY AND FRAUD

Questions

CYBER SECURITY AND FRAUD

Thank you

for

Attending

CYBER SECURITY AND FRAUD

Contact Information

Edmundo Calderon
Chief Internal Auditor
City of El Paso
915-212-1365
calderones@elpasotexas.gov
www.elpasotexas.gov/internalaudit

CYBER SECURITY AND FRAUD