Importance of Cybersecurity Organizational Risk Management

Presented by Michael La Chapelle
MTA IT Security
michael.lachapelle@mtahq.org

MTA Complexity

What is Cyber Risk???

"The exposure of harm or loss related to technical infrastructure or the use of technology within an organization caused by eternal or internal vulnerabilities."

Video Presentation

https://www2.deloitte.com/global/en/pages/risk/articles/cybervideo-companies-like-yours.html

Deloitte.

What could a bad day look like for your organization as it relates to cyber?

Possible Cyber Risk Effects

- Exposure
- Corruption or Destruction of Data
- Disruption of Operations
- Extortion
- Possible Reputational Loss

System and Data Types at Risk

- Customer/Public Facing Systems
- Enterprise Resource Planning
- Payroll
- Health Care and Educational Records
- Desktop/Servers
- Collaboration Tools (Email, File Servers)
- Industrial and Supervisory Control Systems
- Personal, Private, and Sensitive Data
  - Employee, Student, Beneficiary, Family
  - Internal Communications
  - Credit Card
  - Schematics/Designs
  - Legal Documents
- Operational Data that may affect business and consumer decisions

Sony Pictures had a bad day…….

- Hacked November 24, 2014
- Public Release of Sensitive Information (emails, movies, personal info, etc.)
- Destruction of 3/4 of Tech Hardware (PCs, Servers, etc.)

One actual outcome

Breach	Date	Attack Vector
Oracle/Micros	August 2016	Compromised Password
Democratic National Committee (DNC)	July 2016	Compromised Password
Yahoo	December 2016	Multiple – Target was passwords and answers to authentication "security questions
OPM (2 Breaches)	May 2015	Compromised Password
Anthem	February 2015	Compromised Password
IRS	May 2015	Inadequate Authentication (Compromise of Knowledge-Based Questions)
JP Morgan Chase	July 2014	Compromised Password
Target	December 2013	Compromised Password
Apple iCloud	August 2014	Compromised Passwords
Home Depot	September 2014	Compromised Password
Sony Pictures	December 2014	Compromised Password
Heartbleed	April 2014	Compromised Password
1.2B Passwords (Russian CyberVor Hacker Gang)	August 2014	Multiple – Target was passwords to be used for other potential attacks

Cyber Risks Actors

- Internal Malicious
- External Malicious
- Internal Non-malicous
- External Non-malicious

The State of Cyber Risk Management

Even though the number of targeted cyber-attacks is growing by double digits annually, many medium and large-sized corporations still do not devote sufficient resources to cyber risk management.

77%
The percentage of corporations that do not assess their suppliers or customers for cyber risk

68%
The percentage of corporations that have not estimated the financial impact of a cyber attack

43%
The percentage of corporations that have not yet identified one or more cyber scenarios that could affect them

30%
The percentage of corporations that have less than a basic understanding of their cyber risk exposure

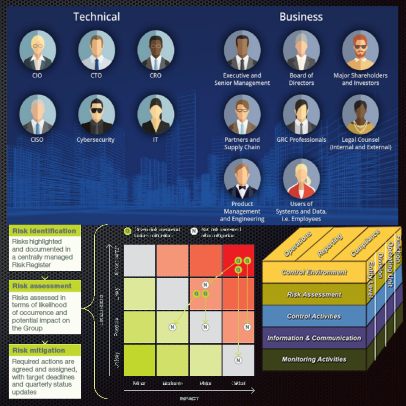
25%
The percentage of corporations that do not include cyber risks in their corporate risk registers

Source: European 2015 Cyber Risk Survey Report, Marsh, Global Risks 2015

Do you know which systems and data are most important to your organization?

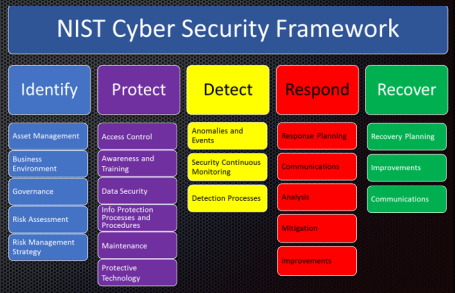
How to Manage Cyber Risks Strategically?

- Discuss Cyber Risks at the most senior level
- Create Cyber Risk Profile for critical cyber assets (assign value)
- Understand Senior Management's tolerance for Cyber Risk and educate
- Coordinate Organizational Strategic Plans with Cyber Investments
- Consider response and mitigation plans (ie. Communication, Cyber Insurance, etc.)
- Monitor and Report



How to Manage Cyber Risk Tactically?

- Focus on critical assets/data
- Identify personnel with access
- Increase Monitor and Detect Capabilities through behavior based methods of abnormal use
- Determine in advance how to mitigate and recover for if occurs
- Internal and External Assessments
- Test and Improve Policies and Controls



Cyber Risk Reality

- Cyber Risks are ever evolving based on business changes and threat landscape
- Controls will need to be continuously re-evaluated
- Cyber education and culture is a must
- Concerns around vendor and contract management around cyber controls (especially in the cloud)
- Cyber security will be a continuous investment
- Good Cyber professionals are in short supply

Questions?

NEW YORK STATE