Boston Chapter AGA 2018 Regional Professional Development Conference Cyber Security

BRANDEIS UNIVERSITY

PROFESSOR ERICH SCHUMANN

MAY 2018

Benchmark

Chinese military strategist Sun Tzu:

- If you know your enemies and know yourself, you will not be imperiled to hundred battles
- if you do not know your enemies, but know yourself, you will win one battle for every battle you lose
- if you don not know your enemies nor yourself, you will be imperiled in every single battle

Cybersecurity Is Top of Mind for Government Leaders

A Call to Action

- Increased responsibilities by managers, executives and senior management to understand and invest in cybersecurity and defend,against attacks
- Attackers work 24/7 to find the undefended
- Cybersecurity team must develop and employ diagnostically relevant tools and methods
- Risks in a digital economy are multi-faced and fast changing
- It's not a question if we will be attacked it's a question when we will be attacked
- According to Kaspersky lab there are 300,000 new malicious files daily
- Cybersecurity culture starts at the top

Cybersecurity Strategy

- ❑ Understand what you can and can not accomplish (know yourself)
- ❑ understand the threat landscape and analyze objectively where we stand among competitors (know your enemy)
- ❑ Understand statutory frameworks

Homeland Security Analysis

1. Cyberspace is particularly difficult to secure due to a number of factors:

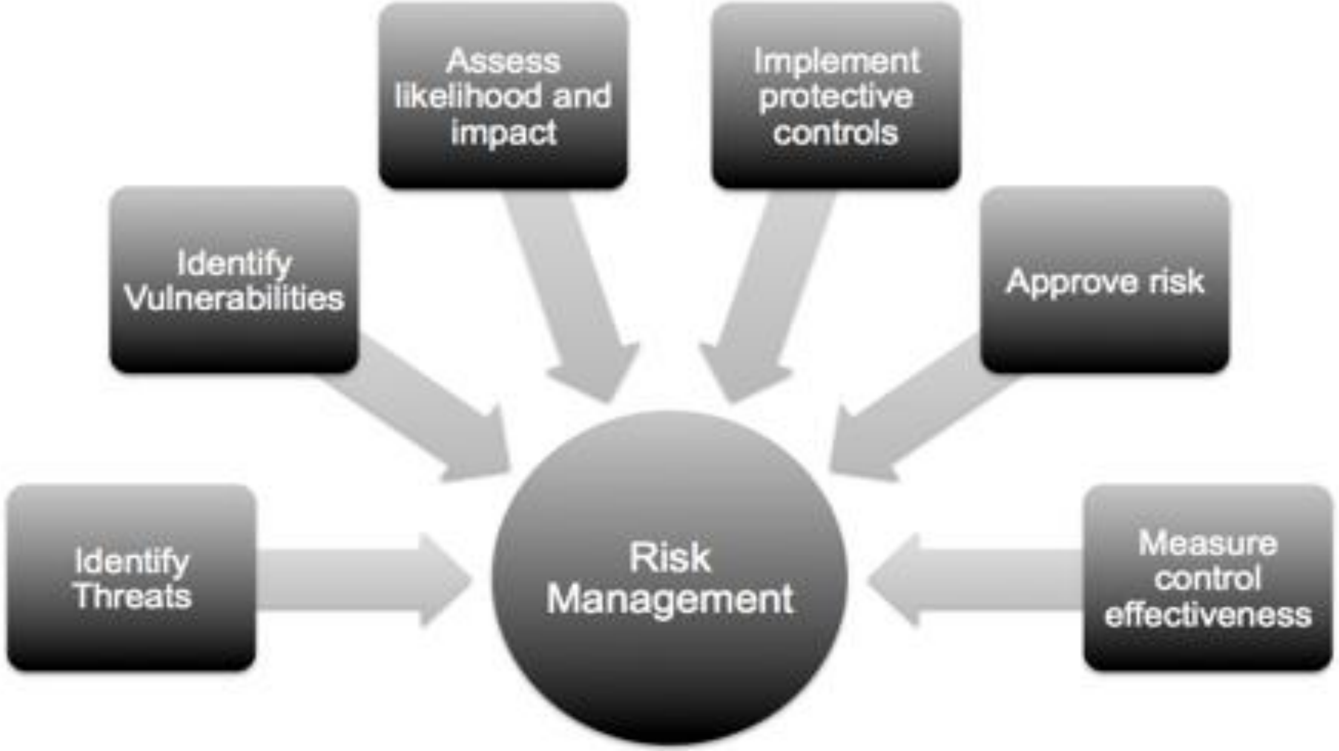
   the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks.

2. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks.
3. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

Homeland Security Analysis

1. Risk Identification:
   a) Assess Evolving Cyber risks
2. Vulnerability reduction
   a) Protect Federal Government Information systems
   b) Protect critical infrastructure
3. Threat reduction
   a) Prevent and disrupt criminal use of cyberspace
4. Consequence reduction
   a) Respond effectively to cyber incidents
5. Enable cybersecurity outcomes
   a) Strengthen the security and reliability of the cyber ecosystem
   b) Improve management of DHS Cybersecurity activities

Find it = Delete it or Protect it


Assess likelihood and impact
Implement protective controls
Identify Vulnerabilities
Approve risk
Identify Threats
Risk Management
Measure control effectiveness

Fifteen Most Critical Controls
Security Information and Event Management (SIEM)

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software on laptops, workstations and servers
4. Secure configurations for network devices, such as firewalls, routers and switches
5. Boundary defense
6. Maintenance, monitoring, and analysis of audit logs
7. Application software security
8. Controlled use of administrative privileges

Fifteen Most Critical Controls

Security Information and Event Management (SIEM)

9. Controlled access on need to know base
10. Continuous vulnerability assessment and remediation
11. Account monitoring and control
12. Malware defenses
13. Limitation and controls of network ports, protocols and services
14. Wireless device controls
15. Data loss prevention

Key Questions
Engagement in Cybersecurity

- Do we include cybersecurity as a core organizational risk requiring appropriate updates in our meetings?
- Do we have someone in the team or advising who is the focal point for this topic?
- Are we satisfied that the our strategies for reducing the risk of security incidents to an acceptable level are proportionate and targeted?
- Do key executives receive key metrics or reporting that present the current state of the security program in an objective manner?
- Is there a policy on securing executive packets and other sensitive material communicated to executives? If not, is there potential exposure from sharing confidential information through personal and professional email accounts and free file-sharing services that are not covered by the organizations cybersecurity infrastructure?

Key Questions for Executives
Identifying the most important Outcomes

With respect to those outcomes occurring:

- Do we know whether and how they are being managed?
- Does our security strategy differentiate them from general cybersecurity?
- Do we assess our threat landscape and tolerance for these matters periodically?
- Are we proactive in identifying and responding to new cyber threats?

Key Questions for Executives
Do we have an Incident Response Plan

- Have key stakeholders supported the development of the plan appropriate to the organizations' scale, culture, applicable regulatory obligations and business objectives?
- Have we thought about the impact specific cyber events can have and whether management's response plan is oriented properly and supported sufficiently?
- Is the plan complemented by procedures providing instructions regarding actions to take in response to specific types of incidents? Do all the stakeholders for a planned response know their respective roles and responsibilities? Is it clear for which events the board should play a key role in overseeing the response efforts?
- Are effective incident response processes in place to reduce the occurrence, proliferation and impact of a security breach?
- Are we proactively and periodically evaluating and testing the plan to determine its effectiveness? For example, does management have regular simulations to determine whether the detective capabilities in place will identify the latest attack techniques?
- In the event of past significant breaches, have we made the required public disclosures and communicated the appropriate notifications to regulators and law enforcement in accordance with applicable laws and regulations?

Summary
6 Ways To Make Smart Cities Future-Proof Cybersecurity Cities

1. ***Prepare*** for the worst—develop a protection strategy and emergency plans, and get outside experts to help;
2. ***Practice***—training and testing and more training and testing and simulations;
3. ***Automate***—implement a continuous adaptive protection, automate the process of detection and response, apply algorithms liberally, including AI and machine learning--based solutions;
4. ***Upgrade***—keep up with attackers' new methods and tools, improve the state of hardware and software including leveraging the cloud and big data analytics and invest in elevating the skill level of the people responsible for cybersecurity defense;
5. ***Share***—raise public awareness, disclose your experiences, and exchange information with other local governments;
6. ***Separate and disinfect***—insert a virtual layer between the internal network and the internet, allowing only for sending commands and showing display windows, and make downloadable files harmless by deleting areas where programs may exist or transform them into safe data, regardless if they are malicious or not