Cyber Risk Management in Today's Threat Environment

August 27, 2015

Kiersten Todt
Roger Cressey
Liberty Group Ventures, LLC

Current Threat Environment

- Hundreds of new malware programs daily, black market for hacking tools continues to grow
- Tactics, Techniques and Procedures (TTPs) being shared by broad range of malicious actors
  - Long range reconnaissance, undetectable attacks, exploitation of mobile devices and supply chain interdependencies
- US is source of many attacks
  - Trend Micro: 28% of watering hole attacks from US
  - NTT report: 56% of attacks on its client base originate from US
- Forensics capabilities now under attack
- Malware complexity is growing: polymorphic software that evolves from machine to machine

Commercial and Federal Sector Challenges

- Use of mobile devices (i.e., BYOD) and web apps increase attack surface
- Social engineering as threat vector
  - Your favorite take out menu is a cyber threat
- Accidental and premeditated insider threats
- Supply chain presents multiple opportunities for adversaries to penetrate networks
  - Third party remote access to corporate systems is a growing problem
    - HVAC; Accounting; Human-Resources Management Systems; Graphics and Data Analytics Functions; Health Insurance Providers; and….Vending Machines

Commercial and Federal Sector Challenges

- IoT and security challenges
  - 2014 NSTAC Presidential report
- Threats of data breach, data loss, data destruction…data manipulation is an emerging threat….DNI testimony
- Security of legacy systems
- Need for better analytics and predictive threat approaches
- Need to invest in cyber before attack, not after
  - More money does not translate into more security

Washington Responds: USG Actions

- Why did the Sony breach prompt USG action?
  - State of the Union
  - EO (“Promoting Private Sector Cybersecurity Information Sharing”)
  - Cyber Threat Intelligence Integration Center
- Greater urge/interest in info sharing legislation…but not the solution
  - ISACs to ISAOs
- What will be the impact of the OPM breach?

Cyber Lessons Learned

- First reports are always wrong! Breaches are almost always worse than originally reported
- Companies do not fully appreciate their cybersecurity interdependencies (i.e., Target/HVAC)
- Employee education remains the foundation of effective corporate cybersecurity
  - Employee behavior (i.e., spear phishing, infected thumb drives, etc.) is a primary corporate vulnerability
  - People, policies, and technology pyramid
- Managing cyber risk means:
  - Assuming you'll be breached; mitigating breach impact
  - Prioritizing and protecting key corporate assets within enterprise
  - Viewing cyber risk as an enterprise-wide risk

NIST Voluntary Cybersecurity Framework

- Called for in Executive Order 13636
- Product of industry, not government
- Creates common language for cybersecurity within and across sectors
- Facilitates behavioral change in organizations
- Applies market-driven approach to cyber risk management
- Encourages organizations to examine and understand key priorities and vulnerabilities
- Supports cyber resiliency within and across sectors

Why Cybersecurity Matters to Senior Executives/Senior Officials

- Regulatory interest is growing; SEC guidance issued on addressing cybersecurity risk (i.e., assessment, strategy)
  - SEC Commissioner Aguilar: “Boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril.”
- Investor activism is growing (i.e., IIS and Target)
  - Senior executives are individually accountable
- Corporate culture is shifting from Prevention to Protection and Resiliency
  - Identify technologies that support corporate strategy to plan for and respond to the inevitable breach
- Breakdown the stovepipes w/technology
  - Technologies need to support integrated cybersecurity strategies, enterprise-wide

Risk Management Steps

- Treat cyber as a risk equal in importance to other business risks (i.e., financial, brand, reputation)
- Use the NIST Framework
- Ensure cybersecurity is a supply chain priority in company's negotiations with vendors and partners
- Education/Awareness
  - Cyber-focused education at all levels: Board, C-Suite, employees, supply chain
- Training and Simulation
  - Within organization/within supply chain
  - Tabletop exercises
- Creative use of proven technologies – CDS for CIP

Contact Information

Kiersten Todt

Roger Cressey

Liberty Group Ventures, LLC

703.647.4110

kiersten@libertygroupventures.com

roger@libertygroupventures.com