Cybervigilance and Cyber-resiliency

By Mark Lanterman[1][2]

In today’s constantly changing and rapidly evolving technological landscape, cybersecurity can seem incredibly challenging to address. No organization is immune to the types of cyberattacks being enacted on a daily basis by external and internal actors alike. From widescale phishing campaigns that seek to target the “human element” of technology to frequently overlooked insider threats, organizations are tasked with understanding cybertrends, risks of cyberattacks to organization goals, and the importance of vigilance and resiliency in constructing and enforcing cybersecurity protocols.

Cybervigilance and cyber-resiliency are cornerstones of strong cultures of security. Developing a culture of security within an organization requires top-down management support, locating and prioritizing priority assets, establishing well-documented communication channels and incident response plans, conducting ongoing security assessments, and investing in education and training for employees.

Key Facts

- Threat actors have four primary motivations for committing cybercrimes, including financial gain, political and/or ideological beliefs, curiosity and fun, or for some emotional benefit. Financial gain is the most common factor, but organizations may be targeted for any one or combination of these reasons.

- The typical profile of a cybercriminal goes far beyond the standard vision
of a lone hacker sitting at a computer in a basement. While lone hackers exist, cybercriminals may be “hacktivists,” organized criminals, or even professional criminals that work for a greater group. Nation states may also be responsible for acts of cybercrime, as demonstrated by the Sony hack of 2014. [3]

- Cyberattacks can damage an organization financially, reputationally, legally, and operationally. The effects of a cyberattack can have both short-term and long-term repercussions that affect overarching goals.

- As technology and cybersecurity strategies strengthen, so too does a cybercriminal’s ability to counteract and create even stronger threats. Malware, social engineering attacks, distributed denial-of-service attacks, advanced persistent threats, and brute-force attacks are all ways that an organization may be attacked.

- Top-down management support is critical in establishing cultures of security that take a proactive approach to cybersecurity, vigilance, and resilience. “Set it and forget it” security protocols are not capable of effectively addressing the types of threat actors and risks that organizations face on a daily basis.

- Incident response teams and clear communication channels for reporting cyberincidents help in relieving the chaos that comes in the wake of a cyberattack, quickens mitigation efforts, and improves public response.

- Cyberawareness within an organization relies on ongoing investment in security assessments, employee training, and education. While top-down support is critical, it must be understood interdepartmentally that cybersecurity is everyone’s responsibility.

- Recommendations:
  - Enterprises must incorporate a cybersecurity approach that takes both reactive and proactive strategies into account.
  - IT Security can no longer be the hub of cyberdefense communication. Establish a corporate communication initiative that begins with the tone at the top and is administered by risk and/ or compliance in partnership with IT.
Establish incident response teams that are charged with handling cyberevents, public response, internal investigations, external communications, and preliminary mitigation efforts.

Act now. Organizations should establish a security baseline and proceed from there. Assume vulnerabilities exist and promote an attitude of “when, not if” when it comes to potential attacks and breaches.

Introduction

The possible financial gains associated with cybercrime is unparalleled, making it incredibly lucrative on both a global and national scale. Historically, cybercrime required knowledge of networks, technology, and how to bypass typical security features. That is no longer the case. Today there are “malware-as-a-service” companies that will create worms, phishing attacks, Trojans, viruses and other malware on demand. Additionally, many individuals work within a group to perform small cybercrime tasks as part of a greater attack.

The cyberworld is unpredictable and constantly evolving. Organizations face threats from a variety of predators. Disgruntled employees can seek to disrupt or embarrass the organization, or sell company trade secrets. Organized espionage groups also actively look to penetrate databases and steal trade secrets and transactional information. Companies that have, or appear to have, a social agenda face the threat of activist dissidents seeking fame and notoriety for their cause through malicious insertions and denial of service.

A recent Ponemon Institute study indicates cyberattacks in the form of data breaches, denial of service attacks, and malware insertions are a daily occurrence— continuing to trend in double digits of percentage growth since 2012. This study assessed 350 global organizations with a purpose of quantifying the high cost of cybercrime. Cybercrimes are costly. The Ponemon study found that the average annualized cost of cybercrime was up 30 percent to $7.2 million based on a range of cost per event from $375,000 to $58 million. However, losses are not just monetary. Reputation damage is the greatest fear among the survey participants.

A recent Experian® sponsored study reports that following a breach or cybercrime event, a company’s reputation with its shareholders, partners and
customers is negatively impacted by as much as 30%. Other areas of concern following a cybercrime event include the adverse impact to share price, employee morale, and external business relations. The 2013 breach at Target® clearly demonstrated the material “blow back” and collateral damage done to a brand, the management team, and the board.

The United States does not have comprehensive legislation related to data security, nor a data breach reporting standard. In the absence of congressionally created cyberlegislation, President Barack Obama issued an executive order[6] in 2013 outlining a framework to reduce cyberrisk to critical infrastructures. The order encourages better communication between government and industry, and fosters the creation of a set of standards, methodologies, procedures and processes. The order dovetails with the dozens of industry-based or activity-based requirements that support an improved risk and compliance posture. These include but are not limited to the joint standard of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC), known as ISO/IEC 27002:2013[7], the Committee of Sponsoring Organizations of the Treadway Commission (COSO) standard for cyber-risks,[8] the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[9] the Internet Engineering Task Force (IETF) Site Security Handbook, RFC 2196,[10] the International Society of Automation (ISA) ISA–99 series,[11] the Federal Energy Regulatory Commission (FERC) Critical Infrastructure Protection (CIP) standards, which are developed by the North American Electric Reliability Corporation (NERC),[12] the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[13] and the Payment Card Industry Data Security Standard (PCI DSS).[14]

With these mounting trends in cybercrime for the majority of us, a cyberwarfare event is not a matter of if...but when.