TechCXO

Product & Technology
Risk & Cybersecurity in the C-Suite

Kirby Winters
Partner – Product & Technology
Information Security
October 2017

Information security is now an enterprise-level concern

- Information Security in modern business has been elevated to the C-suite due to a number of high profile breaches in corporate America and the government.
- IS protection and incident prevention is critical across all levels of an organization.
- Information Security must be championed and communicated across all levels of the organization.

There are numerous major vulnerabilities for a Cyber-Security attack

Attacks can come from external sources and internal breaches. Vulnerability Assessments reveal potential security vulnerabilities or changes in the network which can be exploited by an attacker for malicious intent.

- Security misconfiguration
- Injection vulnerabilities
- Buffer overflows
- Sensitive data exposure
- Broken authentication and session management
- Inadequate reporting to identify hack attempts or breaches
- Insecure third party access to networks

Common terminology will help to communicate key concepts

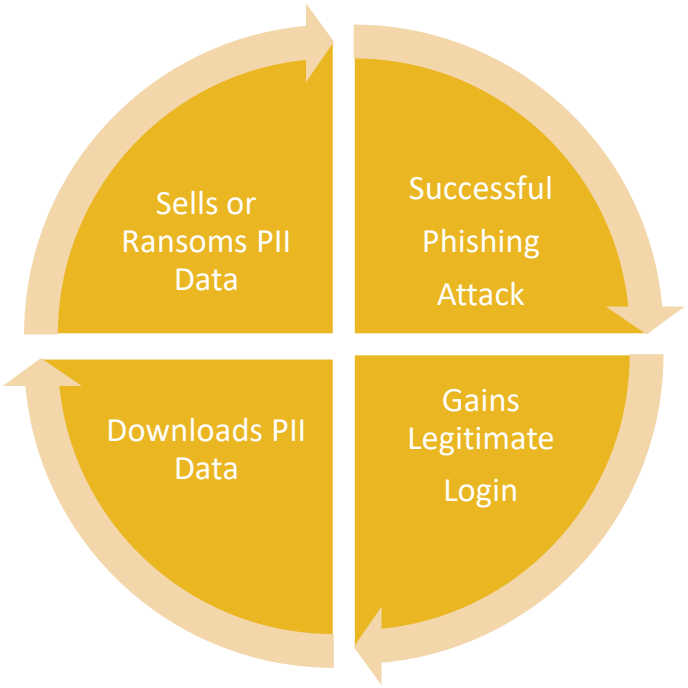
- Information Security - is the practice of defending **information** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- IDS/IPS – Intrusion Detection System, Intrusion Protection System which activity prevents attacks on the network from external sources
- SIEM – Security Information and Event Management system which consolidates devices logs to provide real-time analysis of security alerts.
- MDM and EMM – Mobile Device Management, Enterprise Mobility Management are systems which organize and manage mobile devices in an enterprise.
- VPN – Virtual Private Network used to deliver secure access to a corporate network from external and mobile sources.
- NAC – Network Access Control is an approach to computer security which ensures that mobile or client computers are secure and protected when accessing a corporate network.

Phishing, Spear-Phishing and Whale-Phishing are real world issues every day

Legitimate appearing emails linking to fake websites fool employees and executives resulting in potentially catastrophic hacks

- Ransomware
- Unknown breaches
- Loss of critical data sold on the black market

- C-level executives bear responsibility for cybersecurity risk management



Testing and scanning for vulnerabilities should be an ongoing practice

It is critically important for organizations to test their information security systems and procedures on a regular basis. Organizations are not static and neither are vulnerabilities.

- Vulnerability scans
  - Automated, scheduled, passive, identifies areas for further investigation
- Penetration tests
  - Manual, aggressive, rules out false positives, identifies exploitations
- Risk assessments
  - Detailed analysis and findings, risk scoring, cost benefit analysis of recommendations

Virtually all organizations have either been hacked or will be hacked. Without forensic tools to identify threats, hack attempts and viruses, the organization has no way to respond and remediate the issues. Policies, procedures and tools are needed to track and manage threats and breaches.

- Intrusion Detection/Prevention System (IDS/IPS)
- SIEM (Security Information and Event Management) Reporting System
- Behavior Analysis Tools
- Security Analytics and Incident Forensics Tools

Organizational alignment is required for tight compliance with security standards

- An organization that is dedicated to information security must be committed to it from the CEO down
- Security policies and procedures must be established, be consistent and be reinforced for the entire organization
- Governance of the policies, procedures, hardware, software and maintenance of information security is critical to ensure the most critical security projects are given the appropriate priority and completed

A professional security team applies the SCORE approach to assess clients' security readiness

Category	Eval	Status Description
Organizational Awareness	4	IT is aware, rest of org needs engagement
Security and Risk Management **	3	Minimal policies and procedures
Asset Security **	2	Incomplete security prioritization of assets
Security Engineering **	1	No monitoring or controls for incidents
Communication and Network Security **	3	Basic firewall and application protections
Identity and Access Management**	3	No SSO or NAC for account management
Security Assessment and Testing**	1	No regular vulnerability assessments
Security Operations**	2	Minimal oversight and control systems
Software Development Security**	3	Limited code standards and review
Financial Risk Management	1	No financial metrics aligned to security goals

1: "Needs remediation" 3: "Basic measures in place" 5: "Leading practices in place"
**These domains come from the industry-leading CISSP.

Sample Summary Remediation Report

Security Capabilities	Current	2017 Needs	3 Year Plan
Firewall	✓	✓	✓
SSL	✓	✓	✓
VPN	✓	✓	✓
Employee Screening	✓	✓	✓
IT Security Lead (CISO Role)		✓	✓
Governance & Security Committee		✓	✓
Reporting		✓	✓
Intrusion Protection		✓	✓
Network Access Controls		✓	✓
Incident Response Plan		✓	✓
Network Segmentation			✓
Data Classifications			✓
Single Sign On			✓
Scheduled Penetration Tests			✓
Regular Vulnerability Assessments			✓
Forensic Analysis Tools			✓

Information security is a company wide endeavor that must be evangelized throughout the organization

The following areas are key to a strong information security foundation.

- Strong Governance & Employee Education
- Identity & Access Management
- Mobile & Cloud Security
- Hardened Network Security
- Vigilant Scanning and Reporting

Assessment Overview

An assessment would be performed as remote and onsite investigations of the systems, processes, procedures and reporting for the information security domains of the client. A completed assessment would provide the client with a high-level grade of their information security IQ and remediation requirements.

Deliverables:

- Assessment Engagement (SCORE)
  - **S**ecurity & **C**ontrols **O**perational **R**eadiness **E**valuation
  - Analysis of the client's information security readiness based on the 8 domains of the CISSP program and risk management standards
  - Determination of remediation requirements based on best practices and applicable certifications (PCI, HIPPA, SOC2, ISO 27001)
- SCORE Report and Remediation Recommendations

What can TechCXO offer its clients and partners to mitigate the risks of cyber-attacks?

Offerings:

- Assessment engagement (SCORE)
- Certification preparedness and management
- Fractional CISO
- Governance planning
- System analysis and remediation management

Tools:

- Phishing testing and education
- Vulnerability assessments
- Penetration testing
- Cybersecurity Insurance

TechCXO provides multiple types of engagement offerings to work with any company's needs

- Fractional CISO Services
  - On-going committed leadership role: 20-30 hours per week
  - Team management and executive team participation
- Augmented Advisory Services
  - Directed oversight of special projects: 10-15 hours per week
  - Focused support on critical directives and milestones
- Project Based Deliverables
  - Time and deliverable based work effort: SOC2 Preparedness Engagement
  - General SOC2 Engagement: 150-300 hours
  - Defined scope estimates based on project outputs
- CISO as a Service
  - Monthly retainer providing three key services:
    - Compliance and Governance Management
    - Monthly systems and incidents reporting to Executive Leadership Team
    - On-going vendor and process management of key security procedures

TechCXO

Product & Technology
Risk & Cybersecurity in the C-Suite

Kirby Winters
Partner – Product & Technology
Information Security
October 2017

kirby.winters@techcxo.com
404.993.7719
http://www.techcxo.com