Cybersecurity Introduction

Instructor: Following are some key concepts to aid in a foundational understanding of security in the cyber domain and its role in the enterprise.

Very basically, cyberspace, refers to the hundreds of thousands of interconnected computers, servers, routers, switches, and data transmissions on which critical infrastructures work. With so many services from every sector relying on this digital medium, it is essential to national security.

Cybersecurity encompasses all the technologies, processes, and practices designed to protect cyber elements - equipment, communications, and data - from threats like attacks, unauthorized access, accidents, and natural disasters. Implementing effective cybersecurity measures is an ongoing challenge as devices outnumber humans, technology continues to advance, and the vast amount of data being transmitted and stored continues to expand. Cyber experts and cyber criminals compete to stay a step ahead of the other, regarding that data or more specifically, the information.

Information is an indispensable component of virtually all organizations and their ability to conduct business. Technologies that

produce, store, manage, and protect this information have rapidly evolved and become ubiquitous. Business operations rely heavily on technology such as Voice over IP, virtualization, and cloud services for communications and data handling. Information security, a component of cybersecurity, is a critical integral part of enterprise and risk management. It is the protection of data and the systems it resides on, from risks and focuses on the principles of confidentiality, integrity, and availability.

Referred to as the C-I-A triad, the confidentiality principle is protecting information from unauthorized disclosure; Integrity is the prevention of unauthorized changes; and availability is ensuring the accessibility of the information and resources to authorized users.
The CIA properties applies to data while in the varying states: when information is being worked with or processed, saving and storing the information, and during transmission or the exchange of information. Security measures to protect the confidentiality, integrity, and availability of information in its varying states, requires policies and procedures. This includes laws and regulations for handling and processes. Technology: systems and applications that filter network traffic and enforce access controls, for instance. Finally, education, training, and awareness, a crucial security measure as users are the first line of

defense, and the weakest link in terms of security.

Security properties need protected at the various states information may reside, through security measures. How much, and the type of security measures needed, depends on several factors like the business objectives, the type of information that needs protected, and the available resources. Policies detail business priorities and requirements to support them. Align security with the vision and mission of the organization.

Laws and regulations may require compliance depending on the type of information being handled. There are laws specific to healthcare and finance data for example. The information must be protected from disclosures to avoid fines and other penalties. And performing risk analysis to identify specific threats, the likelihood of occurrence, and potential impact. Carefully defining these variables will help shape security needs.

Enterprise security calls for a layered, or defense-in-depth strategy. There isn't a cyber silver bullet that will protect everything. If an attacker compromises one control, it shouldn't give them the keys to the kingdom. Additional layers provide more detection and deterrence points. Security needs built into all systems at all levels including:

Strong passwords, Access controls, and backups. Application and host hardening. Segmenting networks. Tightly configured firewalls and routers, and use of VPNs. Guards, locks, alarms, and cameras.

Layered security helps support the survivability and resilience of business functions. Survivability, and similarly described risk management concept Cyber Resilience, is the ability to continuously fulfill mission goals, despite the presence of attacks, failures, or accidents.

Three R terms play a role in supporting survivability. Resistance - the ability to repel attacks; for instance, through the use of firewalls that would filter traffic. Recognition - the ability to detect attacks and extent of their damage; an example would be the use of an intrusion detection system that would alert to a packet flood attack with logs revealing if a service was affected. Recovery - the ability to restore essential services, and recover fully after an attack; This may include the use of backup resources and possibly updating access controls.

Achieving survivability and operational resilience requires risk assessment, security controls, along with business continuity and disaster recovery planning activities.

Preparing for worst case scenarios is essential and an ongoing process because the information security ecosystem is ever-changing. New

vulnerabilities and attack patterns are regularly discovered. Attackers may escalate their activities. Underlying technologies continue to advance. New or additional business competitors. Political, social, legal changes. Missions evolve, or change drastically.

Drawing a distinction between security and survivability, security is focused, technical solutions concentrated on specific components whereas Survivability is business driven, long-term interest in the continuity of operations and sustaining the mission of the organization. No individual component is immune to threats; survivability is a risk management approach to sustaining the mission. Cybersecurity in the enterprise is an operational balance. The security measures implemented cannot override the ability to conduct business functions. Electronic communications and working with data - information - are the pillars of most modern organizations. Protecting information resources from threats in a layered approach driven by risk analysis, policy, and legal requirements is a fundamental of cybersecurity.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM18-0098