What is Cybersecurity & What Does it Really Mean?

by **Digital Defense Inc.** | Apr 24, 2019 | **Blog**, **Digital Defense, Inc.**

How Do We Define "Cybersecurity" in Modern Times

Cybersecurity has steadily worked its way from being an Information Technology (IT) problem to being a boardroom priority. But what is 'Cybersecurity' at its core? The cybersecurity definition encompasses the technologies, practices, processes and procedures intended to protect networks, endpoints, programs, applications, and data from attackers intending to cause damage or gain unsanctioned access. The term refers to the both the information security technology involved, as well as the business processes surrounding them.

The familiar term 'information security' has been around since the digital age began, but as infrastructures grew and connected to the internet to meet the requirements of modern day business necessities, as has the need increase protection. The more technology grew with things such as cloud transformation, mobile, Internet of Things (IoT), Bring Your Own Device (BYOD), the more vulnerable companies will become. With those increased vulnerabilities came more regulations, and now information security is no longer a catchall term to fully encompass everything it takes to have a secure IT network, as well as protecting the valuable data that passes through it.

The concept of cybersecurity can be applied in various contexts, from general business operations to firewall technologies, but it can be divided into a few general categories.

- **Information security** – to protect and secure the privacy and integrity of data at rest or at movement.
- **Network security** – to secure a computer network from bad actors that might be a targeted attack or malicious malware.
- **Operational security** – to create and maintain the processes, procedures and decision making for treatment and protecting data assets.
- **Application security** – to concentrate on maintaining the safety of software and devices clear of threats.
- **Business continuity and disaster recovery** – to decide how an organization responds to a cybersecurity incident or breach of data. These are the policies and procedures that dictate how the organization reestablishes control of its operation
- s and information to the same level prior to the event because resources may be lacking post event.
- **Risk Management** – to manage organizational risk in the company's information security program itself, which offers an operative framework for setting the risk appetite and security controls for systems.
- **Security Awareness training –** to address the education of people who often cause security vulnerabilities based on their actions or lack thereof. People can unintentionally introduce a virus or malware to an otherwise secure system if they are not knowledgeable of security best practices, such as deleting suspicious attachments in emails, refrain from inserting unidentified USB drives, etc.

Compliance and Cybersecurity

Compliance plays a large role in cyber security. Compliance departments have traditionally operated separately from IT or security operations teams, but as threats have become wider reaching and more commonplace, privacy and security regulations have increased in number and many come with high penalties.

This caused the modern CISO (Chief Information Security Officer) or ISO (Information Security Officer) role to evolve into focusing on cyber security (not just information security) and compliance of an organization as a whole, breaking down traditional silos between departments to reduce cyber security risks and protect the organization from the inside out and outside in.

Common Information Security Frameworks & Standards that Promote Cybersecurity Best Practices

An information security framework is a series of documented, approved and accepted policies, procedures, and processes that outline how data is managed within an organization in order to reduce vulnerability, thereby increasing assurance in a world plagued by an evolving threat landscape. These frameworks can also guide you towards adhering to various compliance standards.

National Institute of Standards and Technology (NIST)

The NIST Cybersecurity Framework provides a policy guide of computer security practices for organizations in the United States that can enhance their capacity to prevent, detect, and respond to cyber-attacks. This also consists of guidelines, standards, and best practices to achieve cyber security related risk management, which helps to encourage the protection and resilience of an infrastructure.

International Organization for Standardization 27001 (ISO)

Categories

Blog
Chris Graham
CTO: Information General
DDI Labs
Digital Defense, Inc.
Gordon MacKay
Headlines
Mark Bell
Mike Cotton
News
Security
Tom DeSot
Vulnerability Research Team
Zero-Day Alerts

ISO 27001 (formally known as ISO/IEC 27001:2005) is a requirement for information security management systems (ISMS), a framework of policies and procedures that include legal, physical and even technical controls within an organization's information risk management practices. Risk Management plays a large role in an organization's cybersecurity strategy, and many organizations leverage the ISO standards as a framework for security program best practices.

The Payment Card Industry Data Security Standard (PCI DSS)

"PCI security standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with guidance for software developers and manufacturers of applications and devices used in those transactions," as described by the PCI Security Standards Council.*

Needless to say, there are many more and they vary by country, region and even industry.

Types of Cybersecurity Threats

There are many types of cyber security threats that are a thorn in the side of security operations teams.

Malware

Though it comes in many different forms, at its core malware is software designed to cause disorder by disrupting businesses, create network and brand damage, or simply gain unauthorized access to a network.

Advanced Persistent Threats (APT)

An advanced persistent threat (APT) is an attack operation in which a network invader or even teams of hackers establish a long-term presence on a network with the aim of stealing sensitive and private data.

Social Engineering

In information security, social engineering comes in many forms such as phishing attacks. Smishing and spoofing are other common types of social engineering tactics. It focuses on the use of deception and dishonesty to manipulate people into revealing confidential or personal data or material that can be used for fraudulent purposes.

Widely Adopted Cybersecurity Solutions

Vulnerability Management

Vulnerability management is a cornerstone element of any information security program. Vulnerability Management is a continuous information security risk undertaking process. In a strong vulnerability management framework, each process and sub process within it needs to be part of a continuous cycle focused on improving security and reducing the risk profile of network assets. Vulnerability Management includes Vulnerability Scanning, Web Application Scanning and Pen Test Assessment Results. These efforts protect your information assets by evaluating the security posture of the IP devices connected to your computing networks across the globe on an individual IP or enterprise-wide basis.

Network Vulnerability Scanning is used to help determine what is on your network. A vulnerability scanner is capable of quickly, comprehensively and accurately assessing endpoints and servers for operating systems and application vulnerabilities.

Security Information Event Management (SIEM)

Security information and event management (SIEM) hardware and software provide security professionals insight into a record of the happenings within their IT ecosystem. Though SIEM technology has been in existence for more than 10 years, it has evolved from merely log management tactics into new, strategic tactics of analyzing log and event data in real-time to deliver threat monitoring, event correlation and incident response, whereby it can analyze and report on log data. *

Firewalls

Firewalls are often considered the first line or first layer of defense for an organization's network. Digital firewalls are similar to physical firewalls where a device partition that prevents a fire from wandering from one part of a physical structure to another. From an information security perspective, a firewall inserts a kind of filter between the seemingly safe internal network and any traffic incoming or outgoing from that network's connection to the Internet. *

Endpoint Detection and Response

Whether you refer to it as antivirus or endpoint protection, the solution is designed to detect and extinguish computer viruses and malware. Endpoint protection is often considered the third layer of defense in an information security program and protects the actual computer or server that houses the agent. The utility can scan the endpoint manually, be automated or both. Since hackers are constantly creating new viruses, these solutions keep an updated database of virus types and definitions in order to identify them quickly before they wreak havoc on the individual computer and therefore the network.*

In summary, defining cybersecurity in one sentence is difficult to do because it encompasses so many elements. Cyber security definitions will continue to evolve because the threat landscape is always changing. Hackers have more tools at their disposal to attempt to invade a network and steal valuable data with different types of viruses or malware, and they are consistently innovating at a rapid pace. As these new cyber threats continue to emerge, so will cyber security solutions and program best practices.

Resources:

- **https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf**
- **https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html**
- **https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls**
- **https://techterms.com/definition/antivirus**

DIGITAL DEFENSE INCORPORATED

Shrink the Attack Surface™

MENU

- Solutions
- Penetration Testing
- Web Application Scanner
- Security Awareness Training
- Cloud Subscriptions
- Platform
- Technologies
- Professional Services
- Contact Us

CONTACT

Digital Defense, Inc.

9000 Tesoro Drive, Suite 100
San Antonio, TX 78217

Main Line: 888-273-1412
Sales: 888-273-1412 ext. 1
Customer Support: 888-273-1412 ext. 2
support@digitaldefense.com