ESPRESSO TUTORIALS

Julie Hallett

A Practical Guide to Cybersecurity in SAP®

- Cyber risk in the SAP landscape
- How to harden security
- Cybersecurity risk management programs in SAP
- Risk mitigation for threats

Table of Contents

2 Cybersecurity defined

Cybersecurity is not a simple term. It is a concept, program, and process that encompasses data security as a whole. Understanding the holistic nature of cybersecurity will help to develop the process to bring SAP® into a cyber/data security program.

Cybersecurity has been a major buzzword over the last few years, and will continue to be so in the future. It refers to the technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, and unauthorized access, as defined by the U.S. National Institute of Standards and Technology (NIST). It is not simply another name for security, it is the holistic program that wraps around multiple layers of security, compliance, policy and education.

Stop hackers at the network perimeter

Cybersecurity is much more than a way to stop hackers at the network perimeter. It incorporates all aspects of data security, including the largest threat to security—people: employees, contractors, and customers.

A *cybersecurity program* is a holistic processing of requirements and tasks across all layers (see Figure 2.1). It results in a communications chain that manages change across all areas of the IT organization. The goal of the program is to ensure each layer takes into account the other areas impacted by new and emerging threats, and to change implementation.

Creating a holistic data security plan requires a well-thought-out and planned cybersecurity program. In this diagram, the layers of the program are nested and sized according to their importance, level of potential risk, and difficulty to manage. *Network security* receives the most publicity in cybersecurity discussions, but it only plays a small part and depends on the other layers from the perspectives of education, execution, and governance.

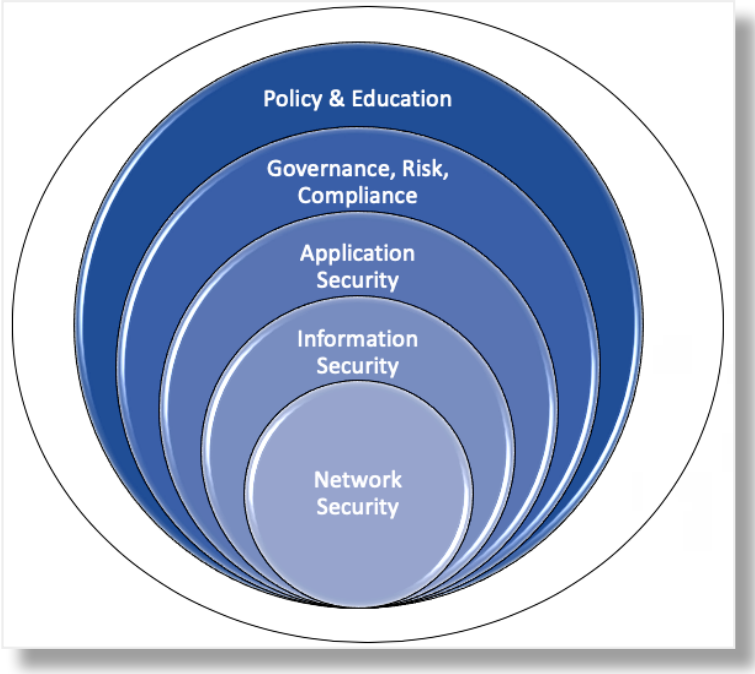

Figure 2.1: Elements of a cybersecurity program

Policy and education is the largest and most complex layer of a cybersecurity program. Definition, socialization and enforcement of policy has legal implications across the entire organization. Security education often requires customization for company divisions, job levels, departments and risk levels, according to the data being managed. This includes the delivery methods for the curriculum, enforcement of education, and recertification on an annual basis. Once employees are educated, regular updates and education about new threats need to be delivered to each employee. The policy and education layer is the foundation of all governance and compliance efforts, applications, information and network security.

Governance, risk and compliance in the cybersecurity program is not a reference to the SAP GRC module (also called Governance, Risk and Compliance). Here, it refers to the processes of managing overall risk to the information, data, intellectual property, and systems that belong to a company. This includes monitoring and enforcing policy, education requirements, threat identification and response, business continuity planning and disaster recovery.

Managing compliance to regulatory requirements for the corporate location and business space means keeping up with all the latest regulations such as the European Union General Data Protection Regulation (GDPR), the NIST CIS (Center for Internet Security) Controls, and the Cybersecurity Maturity Model Certification (CMMC) that are currently being implemented by the US Government as of 2020, as well as many other regulation and certification requirements. The requirements of these regulations permeate through all layers of a cybersecurity program generating new policy, education, application and information security requirements and classifications as well as network security processes.

Application security includes office automation applications, access to network shared drives and data stores, business automation applications, human resources applications, research and development, and many others. Each application has access to data through specific data-storage locations. Access to display or maintain that data needs to be given, while also being careful to provide only the minimum amount of access needed for task requirements. Many companies default to a model where they give their users access to everything they might need at any point in time in order to reduce future access requests and minimize interruption to task execution. Access models are often copied from one group to the next without carefully considering data confidentiality. Designing and implementing application security is time and resource intensive; however, remediation of security after an incident, or for regulatory requirements is much more difficult and can risk business continuity.

Information security includes classification of data into confidentiality tiers. The review and identification of data that is to be restricted is dictated to some extent by regulatory and legal requirements. This includes human resources (HR) data, personally identifiable information (PII), protected health information (PHI) and some company financials. Using this as the only restrictions on corporate information creates risk to the data, thereby impacting a company's trade secrets such as customer lists, price lists, suppliers and supplies, product bills of materials, drawings and assembly details, and new product development. These could be mismanaged and left available to hackers. It is at this level of detail that the intersection between application and information security becomes critical. Unclassified information that is left available to many applications is classified as potential risk. If that data is saved by an employee on an unsecured internet drive (in order to work on it elsewhere), the situation changes from a potential risk to an actual risk, unknown and unmanaged.

These different layers can either reduce or create risk at the network security layer. A breach of policy due to lack of education can introduce new, emerging, or *zero-day* threats to the network. A zero-day threat is a vulnerability that has not previously been discovered or exploited. Zero-day means it is the very first time the vulnerability has been exploited by a hacker. The more access the users have across applications and information stores, the more areas a *threat actor* has to act upon. A threat actor is any person, entity or code that exploits risks or attacks systems. This could include information theft, the planting of malicious code, or the implementation of a robot/bot network application that can launch attacks against other internal targets, external companies, or entities from within the corporate network perimeter.

The use of Shadow IT

Another example of how all the different layers of a cybersecurity program work together to secure corporate data and assets would be the use of *Shadow IT*—the implementation of a technology solution outside the control of the IT department. This occurs when an internal business team decides to employ a cloud service provider to do data enrichment or other services.

When groups or departments decide to implement an application and access to it, without the knowledge or participation of the company's IT team, the standard information technology policies and processes are circumvented, which is a breach of protocol that introduces multiple layers of risk. The use of this service now introduces new data, network and access management risks when it is not in a managed or approved process. This includes the risk that a terminated employee is not removed from their company's online access. If the user is not removed, they will still be able to access the data, and the credentials of that user are then compromised (especially if users are using the same password everywhere). This creates a network penetration risk. Additionally, issues encountered by the service provider are now risks to the company as a whole.

The connection and communication of the five layers of a cybersecurity program are critical for creating a secure, informed technology environment and for managing risk.

3 Using a security framework to manage risk

A framework is a tool used to identify the right questions to ask, and to understand how to organize that information into manageable standards.

3.1 What is a framework?

A framework is a set of guidelines laid out to create standardization across processes. Frameworks are the tools used to implement standards. The terms *frameworks* and *standards* are often used interchangeably. For the purposes of this chapter, we will use them separately with their common definitions:

- *Framework*—a basic structure or system of rules underlying a system; a concept that facilitates decision making
- *Standards*—a rule, principle, technique, process or template designed to provide consistency to planning, development, operation, implementation and governance

A framework is the foundation of questions that guide the creation, understanding, and education of standards and policies. Standards can be self-governing, but the framework provides high level governance to ensure the standards are being met and monitored. Where things get tricky is when there are different frameworks that govern different types of data.

Frameworks are tools to create structure and stability

Frameworks provide a structured set of topics to use to evaluate a system or software. They can be used for any hardware, software, network or data management process to create stability and security.

B Index

R

S

T

U

V

X

Z