# L5 Security Operations

## Module 1: Understand Data Security

Domain D5.0, D5.1.1, D5.1.2, D5.1.3

**Hardening** is the process of applying secure configurations (to reduce the attack surface) and locking down various hardware, communications systems and software, including the operating system, web server, application server and applications, etc. This module introduces configuration management practices that will ensure systems are installed and maintained according to industry and organizational security standards.

### Data Handling

Data itself goes through **its own life cycle as users create**, **use**, **share and modify it**. The data security life cycle model is useful because **it can align easily with the different roles that people and organizations perform during the evolution of data from creation to destruction (or disposal)**. It also helps put the different **data states of in use, at rest and in motion, into context**.

All ideas, data, information or knowledge can be thought of as going through six major sets of activities throughout its lifetime. Conceptually, these involve:

1. Creating the knowledge, which is usually tacit knowledge at this point.
2. Storing or recording it in some fashion (which makes it explicit).
3. Using the knowledge, which may cause the information to be modified, supplemented or partially deleted.
4. Sharing the data with other users, whether as a copy or by moving the data from one location to another.
5. Archiving the data when it is temporarily not needed.
6. Destroying the data when it is no longer needed.

### Data Handling Practices

- **Classification**: classifications dictate **rules and restrictions about how that information can be used**, **stored** or **shared with others**. All of this is done to keep the temporary value and importance of that information from leaking away. Classification of data, which asks the question "Is it secret?" determines the labeling, handling and use of all data. **Classification is the process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality**, **integrity** and **availability**. **Information is then labeled and handled accordingly**. Classifications are derived from laws, regulations, contract-specified standards or other business expectations. One classification might indicate "minor, may disrupt some processes" while a more extreme one might be "grave, could lead to

loss of life or threaten ongoing existence of the organization." These descriptions should reflect the ways in which the organization has chosen (or been mandated) to characterize and manage risks. The immediate benefit of classification is that it can lead to more efficient design and implementation of security processes, if we can treat the protection needs for all similarly classified information with the same controls strategy.

- **Labeling**: **security labels are part of implementing controls to protect classified information**. It is reasonable to want a simple way of assigning a level of sensitivity to a data asset, such that the higher the level, the greater the presumed harm to the organization, and thus the greater security protection the data asset requires. This spectrum of needs is useful, but it should not be taken to mean that clear and precise boundaries exist between the use of "low sensitivity" and "moderate sensitivity" labeling, for example.
  - **Data Sensitivity Levels and Labels**: unless otherwise mandated, organizations are free to create classification systems that best meet their own needs. In professional practice, it is typically best if the organization has enough classifications to distinguish between sets of assets with differing sensitivity/value, but not so many classifications that the distinction between them is confusing to individuals. Typically, two or three classifications are manageable, and more than four tend to be difficult.

  **Highly restricted**: Compromise of data with this sensitivity label could possibly put the organization's future existence at risk. Compromise could lead to substantial loss of life, injury or property damage, and the litigation and claims that would follow. **Moderately restricted**: Compromise of data with this sensitivity label could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned investments or activities. **Low sensitivity (sometimes called "internal use only")**: Compromise of data with this sensitivity label could cause minor disruptions, delays or impacts. Unrestricted public data: As this data is already published, no harm can come from further dissemination or disclosure.

- **Retention**: **Information and data should be kept only for as long as it is beneficial, no more and no less**. Certain industry standards, laws and regulations define retention periods, when such external requirements are not set, it is an organization's responsibility to define and implement its own data retention policy. **Data retention policies are applicable both for hard copies and for electronic data**, and no data should be kept beyond its required or useful life. **Security professionals should ensure that data destruction is being performed when an asset has reached its retention limit**. For the security professional to succeed in this assignment, an accurate inventory must be maintained, including the asset location, retention period requirement, and destruction requirements. Organizations should conduct a periodic

review of retained records in order to reduce the volume of information stored and to ensure that only necessary information is preserved.

Records retention policies indicate how long an organization is required to maintain information and assets. Policies should guarantee that: * Personnel understand the various retention requirements for data of different types throughout the organization. * The organization appropriately documents the retention requirements for each type of information. * The systems, processes and individuals of the organization retain information in accordance with the required schedule but no longer. * A common mistake in records retention is applying the longest retention period to all types of information in an organization. This not only wastes storage but also increases risk of data exposure and adds unnecessary "noise" when searching or processing information in search of relevant records. It may also be in violation of externally mandated requirements such as legislation, regulations or contracts (which may result in fines or other judgments). Records and information no longer mandated to be retained should be destroyed in accordance with the policies of the enterprise and any appropriate legal requirements that may need to be considered.

- Destruction: Data that might be left on media after deleting is known as remanence and may be a significant security concern. Steps must be taken to reduce the risk that data remanence could compromise sensitive information to an acceptable level. This can be done by one of several means:
  - Clearing the device or system, which usually involves **writing multiple patterns of random values throughout all storage media**. This is sometimes **called "overwriting" or "zeroizing" the system**, although writing zeros has the risk that a missed block or storage extent may still contain recoverable, sensitive information after the process is completed.
  - Purging the device or system, which eliminates (or greatly reduces) the chance that residual physical effects from the writing of the original data values may still be recovered, even after the system is cleared. Some magnetic disk storage technologies, for example, can still have residual "ghosts" of data on their surfaces even after being overwritten multiple times. Magnetic media, for example, can often be altered sufficiently to meet security requirements; in more stringent cases, degaussing may not be sufficient.
  - Physical destruction of the device or system is the ultimate remedy to data remanence. Magnetic or optical disks and some flash drive technologies may require being mechanically shredded, chopped or broken up, etched in acid or burned; their remains may be buried in protected landfills, in some cases.
  - In many routine operational environments, security considerations may accept that clearing a system is sufficient. But when systems elements are to be removed and replaced, either as part of maintenance

upgrades or for disposal, purging or destruction may be required to protect sensitive information from being compromised by an attacker.

**Logging and Monitoring Security Events**

Logging is the primary form of instrumentation that attempts to capture signals generated by events. Events are any actions that take place within the systems environment and cause measurable or observable change in one or more elements or resources within the system. **Logging imposes a computational cost but is invaluable when determining accountability**. Proper design of logging environments and regular log reviews remain best practices regardless of the type of computer system.

Major controls frameworks emphasize the importance of organizational logging practices. Information that may be relevant to being recorded and reviewed include (but is not limited to): user IDs, system activities, dates/times of key events (e.g., logon and logoff), device and location identity, successful and rejected system and resource access attempts, system configuration changes and system protection activation and deactivation events.

**Logging and monitoring the health of the information environment is essential to identifying inefficient or improperly performing systems**, detecting compromises and providing a record of how systems are used. **Robust logging practices provide tools to effectively correlate information from diverse systems to fully understand the relationship between one activity and another**.

Log reviews are an essential function not only for security assessment and testing but also **for identifying security incidents, policy violations, fraudulent activities and operational problems near the time of occurrence**. Log reviews support audits – forensic analysis related to internal and external investigations – and provide support for organizational security baselines. Review of historic audit logs can determine if a vulnerability identified in a system has been previously exploited.

It is helpful for an organization to create components of a log management infrastructure and determine how these components interact. This aids in preserving the integrity of log data from accidental or intentional modification or deletion and in maintaining the confidentiality of log data.

Controls are implemented to protect against unauthorized changes to log information. Operational problems with the logging facility are often related to alterations to the messages that are recorded, log files being edited or deleted, and storage capacity of log file media being exceeded. Organizations must maintain adherence to retention policy for logs as prescribed by law, regulations and corporate governance. Since attackers want to hide the evidence of their attack, the organization's policies and procedures should also address the preservation of original logs. Additionally, the logs contain valuable and sensitive informa-

tion about the organization. Appropriate measures must be taken to protect the log data from malicious use.

### Event Logging Best Practices

Different tools are used depending on whether the risk from the attack is from traffic coming into or leaving the infrastructure.

**Ingress monitoring refers to surveillance and assessment of all inbound communications traffic and access attempts.** Devices and tools that offer logging and alerting opportunities for ingress monitoring include: Firewalls, Gateways, Remote authentication servers, IDS/IPS tools, SIEM solutions, Anti-malware solutions.

**Egress monitoring is used to regulate data leaving the organization's IT environment.** The term currently used in conjunction with this effort is **data loss prevention (DLP)** or **data leak protection**. The DLP solution should be deployed so that it can inspect all forms of data leaving the organization, including: Email (content and attachments), Copy to portable media, File Transfer Protocol (FTP), Posting to web pages/websites, Applications/application programming interfaces (APIs).

### Encryption Overview

Almost every action we take in our modern digital world involves cryptography. Encryption protects our personal and business transactions; digitally signed software updates verify their creator's or supplier's claim to authenticity. Digitally signed contracts, binding on all parties, are routinely exchanged via email without fear of being repudiated later by the sender.

Cryptography is used to protect information by keeping its meaning or content secret and making it unintelligible to someone who does not have a way to decrypt (unlock) that protected information. The objective of every encryption system is to transform an original set of data, called the plaintext, into an otherwise unintelligible encrypted form, called the ciphertext.

**Properly used**, singly or in combination, **cryptographic solutions provide a range of services that can help achieve required systems security postures in many ways**:

```
**confidentiality**: Cryptography provides confidentiality by hiding or obscuring a message
**integrity**: hash functions and digital signatures can provide integrity services that all
```

## Module 2: Understand System Hardening

Domain D5.2.1

**Configuration Management Overview**

**Configuration management** is a process and discipline used **to ensure that the only changes made to a system are those that have been authorized and validated**. It is both a decision-making process and a set of control processes. If we look closer at this definition, the basic configuration management process includes components such as **identification**, **baselines**, **updates** and **patches**.

- Configuration Management
  1. **Identification**: baseline identification of a system and all its components, interfaces and documentation.
  2. **Baseline**: a security baseline is a minimum level of protection that can be used as a reference point. Baselines provide a way to ensure that updates to technology and architectures are subjected to the minimum understood and acceptable level of security requirements.
  3. **Change Control**: An update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. A review and approval process for all changes. This includes updates and patches.
  4. **Verification & Audit**: A regression and validation process, which may involve testing and analysis, to verify that nothing in the system was broken by a newly applied set of changes. An audit process can validate that the currently in-use baseline matches the sum total of its initial baseline plus all approved changes applied in sequence.

**Effective use of configuration management gives** systems owners, operators, support teams and security professionals another important set of tools they can use to monitor and oversee the configuration of the devices, networks, applications and projects of the organization.An organization may mandate the configuration of equipment **through standards and baselines**. The use of **standards and baselines can ensure that network devices, software, hardware and endpoint devices are configured in a consistent way and that all such devices are compliant with the security baseline established for the organization**. If a device is found that is not compliant with the security baseline, it may be **disabled or isolated into a quarantine area** until it can be **checked and updated**.

- **Inventory**: Making an inventory, catalog or registry of all the information assets **is the first step in any asset management process**. **You can't protect what you don't know you have**.
- **Baselines**: The baseline **is a total inventory of all the system's components, hardware, software, data, administrative controls, documentation and user instructions**. **All further comparisons and development are measured against the baselines. When protecting assets, baselines can be particularly helpful in achieving a minimal protection level of those assets based on value.** If classi-

fications such as high, medium and low are being used, baselines could be developed for each of our classifications and provide that minimum level of security required for each.

- Updates: Such modifications **must be acceptance tested to verify that newly installed (or repaired) functionality works as required**. They must also be **regression tested to verify that the modifications did not introduce other erroneous or unexpected behaviors** in the system. **Ongoing security assessment and evaluation testing evaluates whether the same system that passed acceptance testing is still secure**.
- Patches: **The challenge for the security professional is maintaining all patches**. **Some patches are critical and should be deployed quickly, while others may not be as critical but should still be deployed because subsequent patches may be dependent on them**. Standards such as the **PCI DSS require organizations to deploy security patches within a certain time frame**. **An organization should test the patch before rolling it out across the organization**. If the patch does not work or has unacceptable effects, it might be necessary to **roll back to a previous (pre-patch) state**. Typically, **the criteria for rollback are previously documented and would automatically be performed when the rollback criteria were met**. The risk of using unattended patching should be weighed against the risk of having unpatched systems in the organization's network. Unattended (or automated) patching might result in unscheduled outages as production systems are taken offline or rebooted as part of the patch process.

## Module 3: Understand Best Practice Security Policies

Domain D5.3, D5.3.1, D5.3.2, D5.3.3, D5.3.4, D5.3.5, D5.3.6

An organization's security policies define what "security" means to that organization, which in almost all cases reflects the tradeoff between security, operability, affordability and potential risk impacts. Security policies express or impose behavioral or other constraints on the system and its use. Well-designed systems operating within these constraints should reduce the potential of security breaches to an acceptable level.

Security governance that does not align properly with organizational goals can lead to implementation of security policies and decisions that unnecessarily inhibit productivity, impose undue costs and hinder strategic intent.

### Common Security Policies

All policies must support any regulatory and contractual obligations of the organization. Sometimes it can be challenging to ensure the policy encompasses all requirements while remaining simple enough for users to understand.

Here are six common security-related policies that exist in most organizations.

- Data Handling Policy: Appropriate use of data: This aspect of the policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization. In addition, some data has associated legal usage definitions. The organization's policy should spell out any such restrictions or refer to the legal definitions as required. Proper data classification also helps the organization comply with pertinent laws and regulations. For example, classifying credit card data as confidential can help ensure compliance with the PCI DSS. One of the requirements of this standard is to encrypt credit card information. Data owners who correctly defined the encryption aspect of their organization's data classification policy will require that the data be encrypted according to the specifications defined in this standard.
- Password Policy: Every organization should have a password policy in place that defines expectations of systems and users. The password policy should describe senior leadership's commitment to ensuring secure access to data, outline any standards that the organization has selected for password formulation, and identify who is designated to enforce and validate the policy.
- Acceptable Use Policy (AUP): The acceptable use policy (AUP) defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action. It should detail the appropriate and approved usage of the organization's assets, including the IT environment, devices and data. Each employee (or anyone having access to the organization's assets) should be required to sign a copy of the AUP, preferably in the presence of another employee of the organization, and both parties should keep a copy of the signed AUP.

Policy aspects commonly included in AUPs: Data access, System access, Data disclosure, Passwords, Data retention, Internet usage, Company device usage

- Bring Your Own Device (BYOD): An organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use. This is sometimes called bring your own device (BYOD). Another option is to present the teleworker or employee with a list of approved equipment and require the employee to select one of the products on the trusted list.

Letting employees choose the device that is most comfortable for them may be good for employee morale, but it presents additional challenges for the security professional because it means the organization loses some control over standardization and privacy. If employees are allowed to use their phones and laptops for both personal and business use, this can pose a challenge if, for example, the device has to be examined for a forensic audit. It can be hard to ensure

that the device is configured securely and does not have any backdoors or other vulnerabilities that could be used to access organizational data or systems.

All employees must read and agree to adhere to this policy before any access to the systems, network and/or data is allowed. If and when the workforce grows, so too will the problems with BYOD. Certainly, the appropriate tools are going to be necessary to manage the use of and security around BYOD devices and usage. The organization needs to establish clear user expectations and set the appropriate business rules.

- Privacy Policy: Often, personnel have access to personally identifiable information (PII) (also referred to as electronic protected health information [ePHI] in the health industry). It is imperative that the organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling of that type of information and are made aware of the legal repercussions of handling such sensitive data. This type of documentation is similar to the AUP but is specific to privacy-related data.

The organization's privacy policy should stipulate which information is considered PII/ePHI, the appropriate handling procedures and mechanisms used by the organization, how the user is expected to perform in accordance with the stated policy and procedures, any enforcement mechanisms and punitive measures for failure to comply as well as references to applicable regulations and legislation to which the organization is subject. This can include national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries such as HIPAA and Gramm–Leach–Bliley Act (GLBA); or local laws in which the organization operates.

The organization should also create a public document that explains how private information is used, both internally and externally. For example, it may be required that a medical provider present patients with a description of how the provider will protect their information (or a reference to where they can find this description, such as the provider's website).

- Change Management Policy: Change management is the discipline of transitioning from the current state to a future state. It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management focuses on making the decision to change and results in the approvals to systems support teams, developers and end users to start making the directed alterations.

Throughout the system life cycle, changes made to the system, its individual components and its operating environment all have the capability to introduce new vulnerabilities and thus undermine the security of the enterprise. Change management requires a process to implement the necessary changes so they do not adversely affect business operations.

### Common Security Policies Deeper Dive

Policies will be set according to the needs of the organization and its vision and mission. Each of these policies should have a penalty or a consequence attached in case of noncompliance. The first time may be a warning; the next might be a forced leave of absence or suspension without pay, and a critical violation could even result in an employee's termination. All of this should be outlined clearly during onboarding, particularly for information security personnel. It should be made clear who is responsible for enforcing these policies, and the employee must sign off on them and have documentation saying they have done so. This process could even include a few questions in a survey or quiz to confirm that the employees truly understand the policy. These policies are part of the baseline security posture of any organization. Any security or data handling procedures should be backed up by the appropriate policies.

### Change Management Components

The change management process includes the following components.

Documentation: All of the major change management practices address a common set of core activities that start with a request for change (RFC) and move through various development and test stages until the change is released to the end users. From first to last, each step is subject to some form of formalized management and decision-making; each step produces accounting or log entries to document its results.

Approval: These processes typically include: Evaluating the RFCs for completeness, Assignment to the proper change authorization process based on risk and organizational practices, Stakeholder reviews, resource identification and allocation, Appropriate approvals or rejections, and Documentation of approval or rejection.

Rollback: Depending upon the nature of the change, a variety of activities may need to be completed. These generally include: Scheduling the change, Testing the change, Verifying the rollback procedures, Implementing the change, Evaluating the change for proper and effective operation, and Documenting the change in the production environment. Rollback authority would generally be defined in the rollback plan, which might be immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.

## Module 4: Understand Security Awareness Training

Domain D5.4, D5.4.1, D5.4.2, D5.3.2

**To reduce the effectiveness of certain types of attacks** (such as social engineering), it is crucial that the organization informs its **employees and staff how to recognize security problems and how to operate in a secure manner**. While the specifics of secure operation differ in each organization, there are some general concepts that are applicable to all such programs.

### Purpose

The purpose of awareness training is to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization. We will be able to align the information security goals with the organization's missions and vision and have a better sense of what the environment is.

### What is Security Awareness Training?

Let's start with a clear understanding of the **three different types of learning activities that organizations use**, whether for information security or for any other purpose:

- **Education**: The overall goal of education is to help learners **improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways**.
- **Training**: Focuses on **building proficiency in a specific set of skills or actions**, including sharpening the perception and judgment needed to make decisions as to which skill to use, when to use it and how to apply it. **Training can focus on low-level skills, an entire task or complex workflows consisting of many tasks**.
- **Awareness**: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.

You'll notice that none of these have an expressed or implied degree of formality, location or target audience. (Think of a newly hired senior executive with little or no exposure to the specific compliance needs your organization faces; first, someone has to get their attention and make them aware of the need to understand. The rest can follow.)

### Security Awareness Training Examples

Let's look at an example of security awareness training by using an organization's strategy to improve fire safety in the workplace:

Education may help workers in a secure server room understand the interaction of the various fire and smoke detectors, suppression systems, alarms and their interactions with electrical power, lighting and ventilation systems. Training would provide those workers with task-specific, detailed learning about the proper actions each should take in the event of an alarm, a suppression system going off without an alarm, a ventilation system failure or other contingency. This training would build on the learning acquired via the educational activities. Awareness activities would include not only posting the appropriate signage, floor or doorway markings, but also other indicators to help workers

detect an anomaly, respond to an alarm and take appropriate action. In this case, awareness is a constantly available reminder of what to do when the alarms go off.

Translating that into an anti-phishing campaign might be done by:

Education may be used to help select groups of users better understand the ways in which social engineering attacks are conducted and engage those users in creating and testing their own strategies for improving their defensive techniques. Training will help users increase their proficiency in recognizing a potential phishing or similar attempt, while also helping them practice the correct responses to such events. Training may include simulated phishing emails sent to users on a network to test their ability to identify a phishing email. Raising users' overall awareness of the threat posed by phishing, vishing, SMS phishing (also called "smishing) and other social engineering tactics. Awareness techniques can also alert selected users to new or novel approaches that such attacks might be taking. Let's look at some common risks and why it's important to include them in your security awareness training programs.

**Phishing** The use of phishing attacks to target individuals, entire departments and even companies is a significant threat that the security professional needs to be aware of and be prepared to defend against. Countless variations on the basic phishing attack have been developed in recent years, leading to a variety of attacks that are deployed relentlessly against individuals and networks in a never-ending stream of emails, phone calls, spam, instant messages, videos, file attachments and many other delivery mechanisms.

Phishing attacks that attempt to trick highly placed officials or private individuals with sizable assets into authorizing large fund wire transfers to previously unknown entities are known as whaling attacks .

**Social Engineering** Social engineering is an important part of any security awareness training program for one very simple reason: bad actors know that it works. For the cyberattackers, social engineering is an inexpensive investment with a potentially very high payoff. Social engineering, applied over time, can extract significant insider knowledge about almost any organization or individual.

One of the most important messages to deliver in a security awareness program is an understanding of the threat of social engineering. People need to be reminded of the threat and types of social engineering so that they can recognize and resist a social engineering attack.

Most social engineering techniques are not new. Many have even been taught as basic fieldcraft for espionage agencies and are part of the repertoire of investigative techniques used by real and fictional police detectives. A short list of the tactics that we see across cyberspace currently includes:

Phone phishing or vishing: Using a rogue interactive voice response (IVR) system to re-create a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted through a phishing email to call in to the "bank" via a provided phone number to verify information such as account numbers, account access codes or a PIN and to confirm answers to security questions, contact information and addresses. A typical vishing system will reject logins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems may be used to transfer the victim to a human posing as a customer service agent for further questioning.

Pretexting: The human equivalent of phishing, where someone impersonates an authority figure or a trusted individual in an attempt to gain access to your login information. The pretexter may claim to be an IT support worker who is supposed to do maintenance or an investigator performing a company audit. Or they might impersonate a coworker, the police, a tax authority or some other seemingly legitimate person. The goal is to gain access to your computer and information. Quid pro quo: A request for your password or login credentials in exchange for some compensation, such as a "free gift," a monetary payment or access to an online game or service. If it sounds too good to be true, it probably is. Tailgating: The practice of following an authorized user into a restricted area or system. The low-tech version of tailgating would occur when a stranger asks you to hold the door open behind you because they forgot their company RFID card. In a more sophisticated version, someone may ask to borrow your phone or laptop to perform a simple action when he or she is actually installing malicious software onto your device. Social engineering works because it plays on human tendencies. Education, training and awareness work best to counter or defend against social engineering because they help people realize that every person in the organization plays a role in information security.

**Password Protection** We use many different passwords and systems. Many password managers will store a user's passwords for them so the user does not have to remember all their passwords for multiple systems. The greatest disadvantage of these solutions is the risk of compromise of the password manager.

These password managers may be protected by a weak password or passphrase chosen by the user and easily compromised. There have been many cases where a person's private data was stored by a cloud provider but easily accessed by unauthorized persons through password compromise.

Organizations should encourage the use of different passwords for different systems and should provide a recommended password management solution for its users.

Examples of poor password protection that should be avoided are:

Reusing passwords for multiple systems, especially using the same password for business and personal use. Writing down passwords and leaving them in

unsecured areas. Sharing a password with tech support or a co-worker.