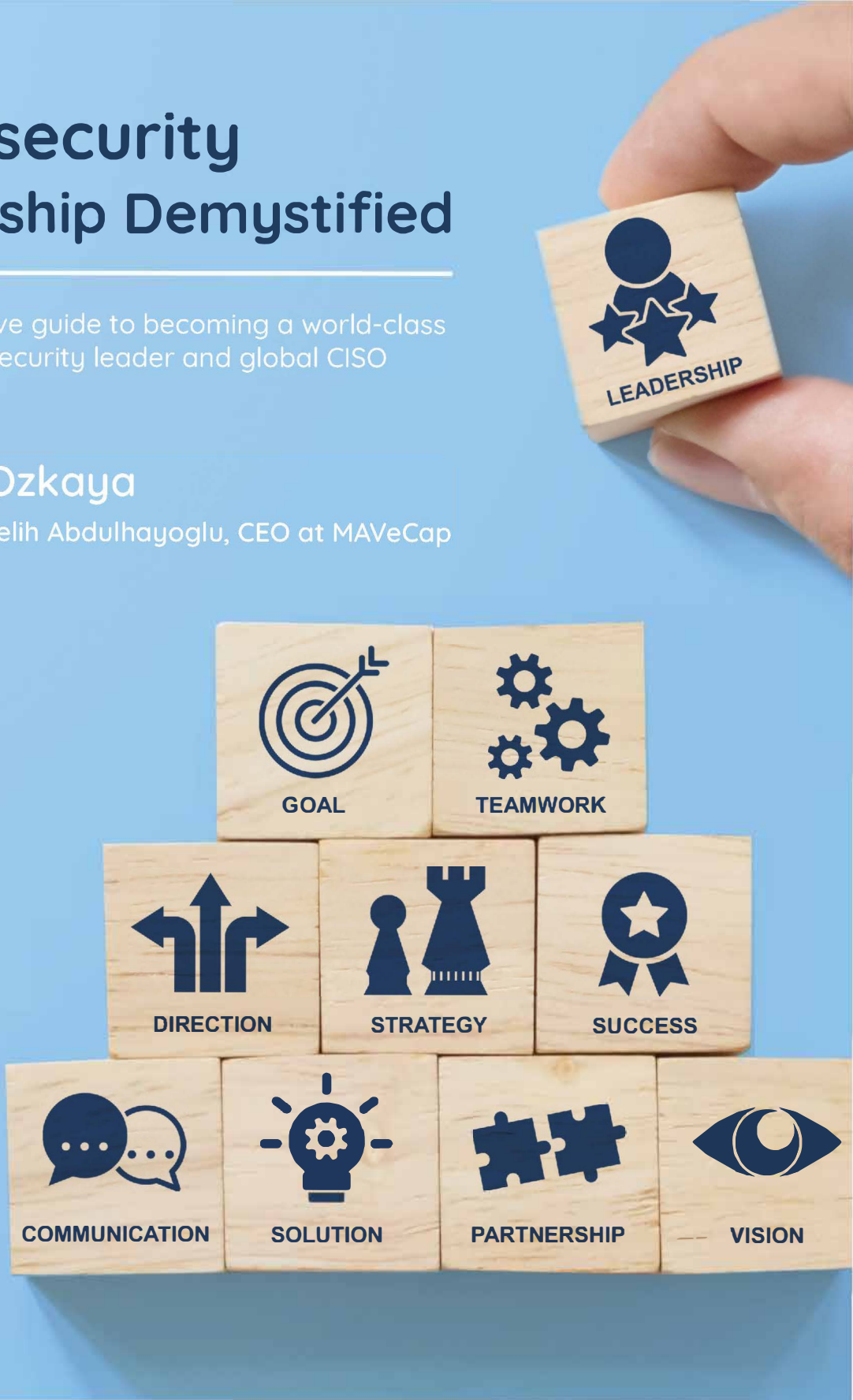
# Cybersecurity Leadership Demystified

A comprehensive guide to becoming a world-class modern cybersecurity leader and global CISO


## Dr. Erdal Ozkaya

Foreword by Melih Abdulhayoglu, CEO at MAVeCap

# Cybersecurity Leadership Demystified

A comprehensive guide to becoming a world-class modern cybersecurity leader and global CISO

**Dr. Erdal Ozkaya**

Packt

BIRMINGHAM—MUMBAI

# Cybersecurity Leadership Demystified



**Group Product Manager**: Vijin Boricha

**Publishing Product Manager**: Mohd Riyan Khan

**Senior Editor**: Shazeen Iqbal

**Content Development Editor**: Romy Dias

**Technical Editor**: Shruthi Shetty

**Copy Editor**: Safis Editing

**Project Coordinator**: Shagun Saini

**Proofreader**: Safis Editing

**Indexer**: Sejal Dsilva

**Production Designer**: Shankar Kalbhor

**Marketing Coordinator**: Hemangi Lotlikar

First published: January 2022

Production reference: 1040122

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK.

ISBN 978-1-80181-928-2

www.packt.com

# Contributors

## About the author

**Dr. Erdal Ozkaya** is a passionate, solutions-focused professional with a comprehensive global background in information technology and cybersecurity.

He worked at Standard Chartered, where he was regional CISO and managing director of the Middle East, Africa, and Pakistan. Before working at Standard Chartered, he was a trusted security advisor and cybersecurity architect at Microsoft, where he perfected the art of mapping customer business problems to technology solutions. He remains committed to delivering accurate, accessible resources to inform individuals and organizations of cybersecurity and privacy matters in the internet age.

Dr. Ozkaya is a collaborative team leader with expertise spanning end-to-end IT solutions, management, communications, and innovation. He is a well-known public speaker, an award-winning technical expert, an author, and a creator of certifications (courseware and exams) for prestigious organizations such as Microsoft, EC Council, and other expert-level vendors with an esteemed list of credits to his name. Dr. Ozkaya is a graduate of Charles Sturt University in Australia.

# 4
# Role of HR in Security

The **chief information security officer** (**CISO**) role is one of the most important management positions in recent times, and organizations are increasingly taking a more serious approach to the hiring of such an executive. A CISO plays an integral role in the **human resources** (**HR**) department. The main reason for their integral role is the fact that internal security is an essential part of organizational security and, more often than not, security breaches result from the exploitation of an internal security weakness.

Social engineering a staff member, obtaining a password from a staff member, or getting a staff member to click on an email containing an intrusive program meant to help a hacker gain access into a system are some of the main methods that attackers use. Therefore, the HR department plays a critical role in ensuring the security of an organization. Hiring practices must ensure that the right personnel is acquired for the position, and hiring processes must also ensure that the hired people have the requisite basic skills to comprehend security policies and help implement some of the security policies meant to keep an organization safe.

A staff member arguably poses a security threat to the system in a similar way to an external worker. Carelessness on the part of staff could help a potential attack to succeed. However, good hiring practices, along with training of staff members, goes a long way in helping CISOs protect their organizations from data breaches.

This chapter addresses the role of CISOs in **HR management** (**HRM**) and intends to show how the HR department is critical to the security of an organization and how CISOs use HRM to improve organizational security. The chapter will address the HRM function through the following topics:

- Understanding security posture
- Exploring human error and its impact on organizations
- Hiring procedures

# Understanding security posture

**Security posture** is a term that refers to an organization's readiness to react to cybersecurity threats. Organizations face several kinds of threats that can lead to data breaches. Attack vectors have increased with the rapid development of technology. Any combination of these vectors can cause security threats to an organization. This has led to increased complexities for CISOs. These challenges may come in the form of **incident response** (**IR**). Security controls, vulnerability testing and management, detection of attacks, recovery processes, compliance, and reporting are some CISO activities that determine the status of a company's security posture. A good security posture increases the chances of an organization succeeding in mitigating security threats that it faces. On the other hand, a bad security posture means that *attack surfaces* are highly vulnerable to attacks, and chances of data breaches are high. The work of a CISO is to ensure their organization has a good security posture.

## Security posture features

To determine the level of security posture for an organization, the following measurements need to be completed:

- Measurement of an organization's ability to detect and subsequently contain attacks
- Measurement of an organization's ability to react and to recover following a security event
- Measurement of an organization's level of security program automation
- Measurement of the visibility that the security team has into all attack surfaces and asset inventory
- Measurement of all the controls that an organization has in place to safeguard an organization from any cyber-attacks

Now that we have listed various security posture features, the next section will provide insights into various **information technology** (**IT**) assets in an organization that are critical to the security situation.

## IT assets inventory

The aim of a security posture is to ensure that all **IT assets** are kept secure from possible threats, either from *internal* or *external* threats. However, it is common knowledge that any security team is incapable of protecting assets they are unaware of. Therefore, CISOs and their teams need to keep an accurate inventory of all the assets that an organization has. Assets in a modern organization include all mobile devices, third-party assets, infrastructure, applications, cloud, or on-premises assets.

It is not enough just to keep an inventory of all the IT assets an organization has—the security team needs to perform a critical analysis of all assets to determine the nature of their criticality in terms of security. This analysis should yield a breach risk level or figure. The breach risk level should then be quantified in terms of **United States dollars** (**USD**) (or any local currency). Quantifying the breach risk serves to calculate the business impact on an organization in case a breach affecting that particular asset occurs.

## Security controls

**Security controls** encompass all the processes in place to detect, prevent, and recover from cyber-attacks. Security controls can generally be categorized into two groups of controls: categorization by *type* or *function*. Under **type categorization**, security controls include *physical*, *administrative*, and *technical* controls. Under **function categorization**, security controls include *preventive*, *detective*, and *corrective* forms of security. The security team needs to have a list of all the controls that their organization has implemented. This list also needs to have a description of the efficiency of each control in helping reduce cyber risks to the organization.

## Attack vectors

An **attack vector** is a term that refers to methods that attackers use to infiltrate or breach an organization's systems. Examples of attack vectors include **man-in-the-middle** (**MitM**) attacks, **phishing**, **compromised credentials**, **ransomware**, and **malware**. Attack vectors can be categorized into types of vectors—those that infiltrate by targeting weaknesses of the security assets, and those that target human users gaining security clearance to access the network.

This chapter will focus more on the second category of attack vectors as they impact decision-making processes as well as hiring practices in the HR department.

## Attack surface

An **attack surface** refers to all the means through which an attacker can gain access to a system using any breach method. It is a description that includes a combination of the asset inventory and the attack vector.

## Automating the security posture

**Automating** security posture management is a critical aspect that ensures an organization's defenses are ahead of those of potential attackers. Many attacks are automated, and attackers use tools that continuously probe the systems for vulnerabilities. With vulnerabilities being identified all the time, it is not enough to have controls for responding and recovering to attacks. The impact of newly identified vulnerabilities cannot be quantified beforehand and, therefore, successful exploitation of such vulnerabilities can be fatal to the continuity of any organization.

## Ways of improving an organization's security posture

In order to improve the security posture of an organization, these three processes must be executed:

1. Analysis of the current security posture.
2. Identification of possible gaps. This is done through assessment of the current security posture.
3. Taking measures to ensure that identified gaps are addressed.

After listing ways to improve the security posture, we will address how to assess an organization's security posture in the next section.

## Assessing an organization's security posture

The *assessment* of an organization's security posture is the first step toward addressing cybersecurity risks and attaining the required levels of compliance. Without an understanding of the current processes, it is not possible to tell exactly which vulnerabilities affect a business, how these vulnerabilities can be exploited, the risk involved in case these vulnerabilities are exploited, and the business impact of these risks. Without this knowledge, a business will be running blind in an increasingly *dangerous IT landscape*. In assessing the security posture, the following list of questions needs to be asked. A CISO and their team should be able to answer the questions posed:

1. How safe is our organization?
2. Does our organization have the right cybersecurity strategy to defend the company's IT assets?
3. How good are the security controls we have in place?
4. Are we in a position where we can accurately measure our cybersecurity resilience and breach risks for all our assets?
5. What is our level of vulnerability to possible attacks and potential data breaches?
6. Do we have a vulnerability management program, and how effective is the program?
7. Can we effectively evaluate the various business risks as well as benchmark the various risk owners in the business?
8. Do we have an adequate process through which our reporting of the security posture is made to the board of directors, including a discussion around the security posture?

On answering all these questions, the organization should be in a position to fully understand the current situation of the security posture and, based on the understanding, make adequate plans to address concerns as well as future needs.

## Important steps in security posture assessment

Effective security posture assessment is completed in three key steps, and we will look at this in the next few sections.

## Determining an IT asset inventory

Organizational assets include all the gadgets that have access to the business' network and data. In inventory-taking processes, the security team needs all the details of all these assets. These details should comprise up-to-date information about the assets as well as a deep understanding of the assets, which includes all risks associated with the asset. Needed details at this stage include the following:

- Categorization of all assets based on location, type of asset, the role of the asset in the organization, and whether it connects to the internet or not.
- Determining the criticality of each asset.
- In-depth information details of all software and hardware details for the asset such as users, ports associated with the asset, and services linked to the asset.
- Asset licenses. Details of all licenses and ensuring that the assets are running up-to-date license software and adhering to the business's security policies.
- Ensuring that actions are triggered to automatically alert security personnel when an asset deviates from organizational security policy procedures.
- Decisions on which assets to decommission and stop using when they are no longer up to date or no longer usable.

Tracking and keeping a detailed record of assets is a basic process that is integral to maintaining security standards and is a requirement for most internal regulations and standards such as the **Health Insurance Portability and Accountability Act** (**HIPAA**) and **Payment Card Industry** (**PCI**) standards. With an accurate list of organizational assets, the security team can create effective plans that cover all assets.

## Mapping all attack surfaces

An **attack surface** is any point in an organization's network where an attacker can gain access to the network. Essentially, these are data points where attackers can potentially access and compromise an organizational asset.

## Understanding cyber risk

The last step to security posture assessment includes an understanding of the business risk of attack surfaces. **Cyber risk** is the potential loss that can result from a successful cyber-attack. To accurately determine the cyber risk, the following factors need to be considered:

- The criticality of the asset

- The threat level
- The severity of the vulnerability of that particular asset
- Risk-negating effects as a result of certain security controls

Understanding the security posture and subsequently addressing the identified issues ensures that an organization remains in control of the security aspects and greatly minimizes the business risk while simultaneously increasing the chances of business success. A CISO plays a critical role in an organization with their carefully recruited team of security experts. Users pose as much a security threat to an organization's system as infrastructural weaknesses. Therefore, for CISOs to ensure good security postures, they need to ensure that the HR department hires the right personnel and fires or penalizes people in breach of the various security protocols meant to protect an organization's security posture.

This section has addressed the important role of a CISO in guaranteeing a good security posture that ensures the minimization of business risk. The next section will address the second key HRM function of human error and the impact this has on organizations.

# Exploring human error and its impact on organizations

Employees pose a big threat to the security of an organization. While many organizations have invested heavily in setting up perimeter walls to keep intruders out, it is the *insiders* that remain a major problem as far as the security of an organization is concerned. Insiders that pose a threat to an organization range from former employees, current employees, business partners, interns, customers, to contractors. Arguably, they pose a greater threat because of their knowledge of the systems and because of the trust the organization may have in these employees. More often than not, it is insiders that either cause an attack themselves or through whom an attack is possible. Laxity on the part of organizations in terms of security policies involving employees is well documented. In 2001, for instance, the **Federal Bureau of Investigation** (**FBI**) revealed that a Russian spy had worked within their ranks for 20 years and had helped the *Russian intelligence services* to infiltrate the US's systems for years without the knowledge of the FBI administration. The news was a major lesson not just for the FBI but also for other organizations that hold sensitive information that may be a target for malicious attacks. Therefore, for the security team to be effective at keeping an organization safe, the focus should not only be on internet-based attacks; insiders, especially employees, should also be monitored.

## Preventing insider security threats

Insider threats are a major threat to an organization. Firewalls and other forms of authentication can only help keep outsiders out. However, there are several means of dealing with this threat. Some examples of effective ways of preventing insider threats include the following:

- **See something, say something**: Encouraging employees to report fishy behavior they have witnessed among their colleagues because all employees are a vital component of a company's security posture. Employees should also be encouraged to conduct a self-audit of their activities to determine whether they are a risk to the company or whether their actions help increase the risk aspect.
- **Educating employees**: This will help prevent an accidental breach of security. However, it will not help prevent an intentional data breach.
- **User access hygiene**: This means that all user accounts should be evaluated. All dormant and orphaned accounts should be deleted from the system—for instance, temporary accounts may be created for purposes of a given project that may provide users with access to sensitive data. After completion of such a project, these user accounts are no longer necessary and should be eliminated from the system.
- **Strong authentication**: Weak authentication procedures just help attackers infiltrate the system. The system should require employees to use strong passwords as well as **multi-factor authentication** (**MFA**) to safeguard their user accounts.
- **Third-party access**: Control third parties such as vendors, contractors, and consultants whenever they are accessing the company's facilities. Their movements should be monitored, and they should be provided with an escort while visiting a company's facilities.
- **Sentiment analysis**: This refers to the use of behavioral analysis techniques to handle potential threats. For instance, erratic employee behavior should be considered a potential risk to the company and, therefore, remote logins and other security credentials should be limited or monitored.
- **Compromised accounts**: An organization should invest in the detection of compromised accounts. Compromise may result from actions such as malware downloads. Such accounts should then be restricted from accessing the system, and this will probably help prevent a major incident.
- **Data exfiltration**: Monitoring data and access to data within a company's servers should help prevent successful attacks from insiders. For instance, file movement from servers to a file-sharing site is an irregular process and such actions should raise an alert, with automated action taken to prevent these actions from completing.

- **Privileged access abuse**: Stopping privileged access abuse will help stop insider threats. Tools that monitor privileged access users and control changes to sensitive information will help reveal efforts to abuse privileges and hence reveal possible attacks.
- **Monitoring user behavior**: The monitoring of employees is the first and most obvious means of protecting the system from possibly threatening a company's informational assets.

This topic has addressed various components of the HR factor in organizations and how it affects the security situation. The next section will provide insights into hiring procedures and how integral these are to security policies imposed to improve the security posture of an organization.

# Hiring procedures

Recent research finds that more than half of all data breaches occur due to **human error**. It is therefore critical for CISOs to establish a system that reduces human error and its impact on their organization's security posture. Responsibilities begin with setting the right criteria and mechanisms to hire employees with knowledge and awareness of security risks facing their daily work routine. These include, among others, the following:

- Verification checks for job candidates
- Security education and training program
- Policies for **identity and access management** (**IAM**)

**Hiring procedures** are an essential function of the HR department. Hiring procedures ensure that an organization not only gets the most competent job applicants out there but also that employees fit the mission and vision of an organization. Some of the factors that an organization seeks in job candidates are school qualifications and relevant experience. However, to find certain types of employees that fit an organization's vision, virtues such as integrity, honesty, intelligence, determination, and loyalty may be considered during hiring.

With the increased use of technology and its increasing importance for security, a CISO must influence all aspects of an organization. The HR department is no different. A CISO needs to help ensure that the HR department gets the right people into the business that can help safeguard the system. Ideally, staff should have some IT knowledge to appreciate the importance of IT security and the application of various security policies. It is harder for non-IT candidates to understand the impact of their actions and reasons for the implementation of certain security policies that may seem overly cumbersome.

Some of the reasons for the involvement of CISOs in hiring practices will be covered in the next sections.

## Performing verification checks for job candidates

It is absolutely critical for an organization to get employees that can pose as little a threat to the security of business information assets as possible. Verification checks are important as they ensure that those hired are people without questionable character and that their intentions are clean. Ideally, people whose backgrounds are unclear should be avoided. People whose backgrounds show a history of dedication to work and family should be positively reviewed, and they have an increased likelihood of employment.

In case it is not possible to perform a thorough verification of job candidates, then an external bureau that specializes in background checks can be used. The aim is to ensure that a company employs people of unquestionable character. Such people can help enhance the security posture of a company by adhering to security policies.

## Security education and training

**Security education and training** is a function that requires both CISO and HR department input. Employees may be hired to work within various departments but need security training, as all the sectors of a business can prove to be an attack surface. Security operations apply to all sections of a business and, therefore, all employees need to be educated on the security policies and the reasoning behind the policies. Employees who understand the reasons behind the security policies are more likely to adhere to these policies. However, a lack of education will lead to more accidental security incidents by employees who are either resistant to the security policies or those who see those policies as bothersome company regulations.

Whenever CISOs implement new security features or installation of new systems, employees need to be educated on the new systems and their role in ensuring the system is safe from malicious attackers. Therefore, the CISO, along with the HR department, will work toward preparing education and training sessions for employees to teach them of their requirements in the new system and their obligations. An update in employee security obligations needs staff to be educated. Due to frequent system upgrades, educational and training programs should be run as often as possible.

CISOs should work in unison with the HR department during hiring periods to ensure that new employees are enrolled for training immediately before they can start using the system. Interns should also have a training program to ensure that everyone who works with the business system is aware of the security needs and their role in ensuring that security requirements are met.

## Security risk awareness

CISOs have an important role in improving the security posture, and this is only possible with improved security awareness among employees. Employees pose a security threat to an organization and security controls are often put in place to ensure a company is protected from insider actions. However, security controls are not foolproof, and increasing the security awareness of employees is the best way of reducing business risk. As mentioned before, the use of training and educational activities is the main way of increasing the security awareness of employees. The hiring of employees that are technology-savvy is another way of ensuring higher security awareness among a company's employees. Clearly laying out consequences for breach of security controls is another great way of improving security risk awareness. If employees know of the consequences of security breaches and they feel this will result in termination, suspension, warnings, and fines, then they will engage in due-diligence activities.

Hiring practices should adhere to security protocols. The CISO should work with the HR department in creating job requirements and hiring procedures that ensure security awareness is an important factor that should be tested among potential job applicants. A job applicant with a high level of security awareness should be considered. The importance of security awareness has necessitated increased vigilance and hiring practices that ensure hired employees are aware of security threats and that they actively participate in ensuring they are not part of the problem.

## Organizational culture

The **organizational culture** is an important aspect of security for an organization. Usually, employees have a certain culture that influences most of their actions and, more often than not, management has an important role in creating this organizational culture. Users may know the right thing to do but fail to do it—for instance, users may know that they need their security cards to get into some parts of the building but may use their colleagues' after misplacing their cards. More often than not, such habits create a culture of insecurity in the long run as they open up loopholes that can be exploited by malicious individuals.

CISOs need to stamp out such a dangerous organizational culture and encourage the strict implementation of security controls and policies. This can be done through warnings, unscheduled audits, camera monitoring, and terminations. Having an organizational culture that is rooted in security measures is an effective way of improving the security posture of an organization. Regular education and clearly pinned security protocols to remind workers of the protocols should enhance awareness and create a culture rooted in a good security posture. Another effective means of maintaining security awareness is job rotation to ensure that an employee does not retain one workstation indefinitely for them to grow complacent and engage in sub-optimal security measures.

This section has provided insights into the employee role and how they can contribute toward increasing the threat risk to security. The next section will handle policies created by security leaders to address both internal and external security threats.

# Policies for IAM

Policies are a crucial aspect of the security posture of an organization. Policies are internal regulations that are created in accordance with the unique needs of an organization's business activities. In this section, we will address policies that are crucial to ensuring denial of access to information assets within an organization without proper authorization.

## Implementing security policies

**Security policies** are the main solution to limiting the kind of damage possible from an insider threat. They reduce the carelessness of employees and reduce the chances of attackers taking advantage of complacency from employees to access the system. Security policies should include clearly laid-out procedures that employees should follow for the security of an organization. In addition, the consequences of breaching any of these policies should be clearly outlined. Employees should understand that their actions can put the business at risk, and so they should follow security guidelines as instructed to ensure that the business protects its assets from malicious attacks. Consequences could be in the form of legal liability, fines, suspensions, and termination of contracts based on the extent of the breach or the likelihood of damage from their actions.

Security policies should outline the limitations of all employees, the kind of data they can access, and the consequences of accessing such data. Mishandling data and accessing data an employee should not be handling is a red flag that should put such an employee in line for serious consequences. Spelling out the consequences also helps to eliminate the chance of unfair penalties being applied to employees if they are in the wrong. The HR department handles employee issues, and these guidelines should be part and parcel of the employment contract that an employee signs when accepting employment. Also, whenever there is a change of security policies as a measure to improve security or in response to the installation of new security systems or guidelines, the employees should be informed and required to read and agree to the changes in their contractual obligations.

## Physical security

**Physical measures** to improve security are a simple yet effective way of keeping insiders in line and a system safe from mishandling from employees. Every employee has their station of work within an organization. Sensitive locations such as servers that house sensitive information should be kept in the furthest room in the building to make it harder for people to access it, and this applies to both customers and employees. Only authorized personnel should be able to access the room. Physical restrictions from accessing the servers should help keep the servers secure and safeguard against tampering.

Some of the available technologies to implement physical safeguards include the following:

- **Two-factor authentication (2FA)**: Using key cards to access certain rooms is a common physical security measure to keep unauthorized people out of certain areas. However, with trust among employees, one of them can borrow a card or use another's card to access certain areas of the building they are not mandated to access. The use of 2FA helps increase a layer of security that will make it harder for people to access certain restricted areas of the system.
- **Biometric authentication**: Fingerprint and face scanners are common biometric authentication systems that help enhance physical security. This option is possible for large and profitable organizations given the expensive nature of installing such systems. Organizations that can afford this kind of system are more reliable compared to simple key card use that can easily be exploited internally.

- **Lock and key**: The simplest form of security that does not require advanced technology, yet it remains an effective layer of security in modern times. Thieves and kleptomaniacs among employee staff can steal sensitive information or unsecured pieces/hard copies of sensitive data. Therefore, employees should have lockable drawers in their workstations to safeguard the sensitive data they are responsible for.

CISOs have an important role to play in the HR department toward ensuring personnel security among staff members in an organization. Personnel security is a priority engagement and is made possible through the implementation of various procedures that guide various business functions with contractors, vendors, and consultants. These procedures also include hiring practices.

## General safety procedures

To ensure a safe business environment, an organization should engage in activities such as the following:

1. **Physical security incident responses**: An organization needs to have procedures and policies that outline activities that the company's personnel should engage in in the event of personnel safety concerns. One way of ensuring employees are safe is to conduct employee training.
2. **Training and drilling**: Employees should be aware of the possibility of physical security threats to their organization that may target the organization's information assets and they should receive training and practice on how to respond to such cases. Training and drills should be done to practice for such things as storms, fires, pandemics, active shooters, and so on.
3. **Succession planning**: A company should have plans in place that detail the succession procedure regarding the person that should take over the management of the company in case a person(s) in management is fired or is incapacitated. Such procedures ensure the safety of information assets, as only select staff will be accorded access to these assets.
4. **Traveling**: It is expected that organizational leaders may have to travel from time to time to other regions of the country or world. Safety procedures may include the use of third-party security services or escorts. In such cases, the procedures should outline how these services should be contracted to ensure the security of the organization and eliminate the possibility of leakage of such information. Additionally, several senior staff can travel on separate airlines or different mediums of transport to reduce the risk of an organization losing multiple members of the management staff in case of an accident.

5. **Operational security**: This form of security is often referred to as **OPSEC**. OPSEC requires that personnel should learn to keep sensitive information to themselves and learn what to give away in case they are conversing with other people wherever they are. OPSEC works on the assumption that attackers can glean sensitive information that can enable them to successfully attack an organization by piecing together several strands of sensitive information. Practicing good OPSEC means that personnel should limit the information they share regarding their work with other people, and this includes their fellow workers.

## Employment procedures

The management of the life cycle of employment processes is part and parcel of personnel security. Some of the procedures that should be managed to ensure personnel security include the following:

1. **Employment screening procedures**: Before hiring employees, an organization needs to have in place employment procedures that they follow when employing staff members. These procedures ensure that hired staff members are suitable for the roles they will play in the organization. These procedures will include drug screening, background checks, credit checks, and security clearance requirements.
2. **Employment policies and agreements**: To ensure personnel safety as well as safety of an organization from threats emanating from employees, before hiring them an organization needs to ensure that they sign the following documents: **non-disclosure agreements** (**NDAs**), ethics agreements, code of conduct policies and conflict of interest policies. These documents ensure that employees follow the expected behavior, and it helps protect the information assets within an organization.
3. **Employment termination procedures**: These are safety procedures followed when an employee is fired or has their contract terminated. These procedures encompass such actions as completing an exit interview, reviewing the NDA, revoking company **identifier** (**ID**) badges, returning company keys and any other company assets, disabling user accounts, changing passwords, and escorting the individual off the premises.

## Vendors, contractors, and consultants – procedures

Physical security procedures do not just deal with matters pertaining to employees—they should also have provisions for third parties that visit an organization's facilities. These third parties include such people as vendors, contractors, and consultants. Some of the procedures that should guide their visits to organizational facilities include the following:

1. Escorting visitors while they are within the premises of the organization.
2. Verifying their identities and ensuring that there are proper access-control mechanisms in place.
3. Verifying visitors' licenses and other forms of identifications they may have.
4. Asking visitors to complete a sign-in sheet as well as sign out when they leave the facilities.
5. Issuing visitors with a name badge and requiring them to always carry these badges while within the premises.
6. Ensure that appropriate agreements with these visitors are in place.
7. Ensuring they sign NDAs.
8. Ensuring that these visitors are screened properly before engaging them on a contractual basis.

While this section has provided a list of procedures that should be used to handle vendors, consultants, and contractors when they visit an organization, the next section will address the issue of hiring practices and how to ensure they contribute toward tightening the security situation.

## Tight hiring practices

A background check on new staff members is an effective means of keeping internal systems safe. An attacker can pose as an employee to gain access to a system from within—therefore, investing time and resources into performing background checks is an important security measure that helps a business safeguard its systems. Background checks can be expensive, and an organization may not have the resources to perform them effectively. In this case, it is advisable to outsource these services to professional security firms that can conduct effective background checks to reveal more information than the HR department can access. Background checks can be performed not only on employees but on business partners and vendors as well. Before engaging a vendor or outsourcing work that may require granting access to your systems, an organization needs to perform background checks to assure them of the integrity of business partners or vendors.

## Using strong authentication mechanisms

Passwords can be cracked. With increased hardware and software capabilities being readily available to people, it has become easier for this to happen; therefore, it is no longer prudent to use simple passwords. Employees should be educated on the need to use strong passwords for their computer systems. In addition, they should be discouraged from using the same password they use on personal devices and online accounts to safeguard company assets. Attackers focusing on an employee will hack easier accounts to determine a password used elsewhere and try the same password, as many employees prefer easy passwords they have used over the years. These habits should be discouraged as they put a business at enormous risk. MFA is one of the solutions that can be used to enhance password security.

## Securing internet access

Companies can help secure their computers from access to certain sites and hence keep their employees in check. Group policies enable management to set configuration details on company computers that limit an employee from the kind of sites they can access while working with company systems. An organization can limit internet-based services to the company website and a handful of other sites that are considered necessary for an employee's work. This will limit employees from accessing all kinds of sites while using company devices that could provide an avenue for potential hackers targeting the company employees. Accessing company files should be restricted among employees and should be allowed only on a need-to-know basis.

## Investigating anomalous activities

Log data is an important source of data that can be used to perform investigations into network activity. For internal users, the internal **local area network** (**LAN**) should be a good source of log data that can be used to investigate any anomalous activities among company staff. Based on recent investigations of insider data breaches, it has been shown that insiders often do not attempt to cover their tracks as they do not seem to expect to be caught. While external hackers go to great lengths to cover their tracks, insiders do not do the same. However, it is important to note that logging of data among non-domain controllers such as **New Technology** (**NT**)/**Windows 2000** (**Win2K**) servers is often disabled by default, and this proves difficult during investigations due to insufficient log data on internal LANs. However, enabling this system enables the internal logs to keep data of internal staff operations, which can then be analyzed in case of investigations or in an attempt to detect anomalous activities.

## Refocusing perimeter strategies and tools

In most company security strategies, the focus is on internet-based attacks and keeping malicious attackers away. Perimeter tools to keep external attackers away are vigilant and often do a thorough job. However, the same cannot be said of internal systems. By refocusing the perimeter wall strategies toward internal mechanisms, a lot can be achieved, and internal threats averted. Internal patching is one such strategy that is used on the external perimeter wall to safeguard email and web servers on the internet domain; however, it is rarely done on internal systems. Applying such strategies to internal systems will dramatically increase the safety of these systems and reduce the risk of internal damage.

In addition, vulnerability assessment for internal systems—a strategy that is commonly used to safeguard external-facing services—can be used on internal systems as well. The assessments can be done by scanning all critical servers that are used by employees to determine any weakness that can be exploited by internal staff and by taking the necessary steps to safeguard the systems from exploitation of vulnerabilities.

## Monitoring misuse of assets

In addition to having security policies that employees need to follow to ensure a good security posture, monitoring of employees is often a requirement that radically improves the security posture. The use of video cameras and keystroke logging are examples of additional monitoring mechanisms that can be used in this case. However, some of these measures can be illegal—for instance, they can be an invasion of privacy, and the company can be sued and suffer reputational as well as financial damage if found in breach of privacy laws. Therefore, any monitoring should be done within the confines of the law. Web content filters can be used to monitor and restrict employees' access to websites such as competitor websites, pornographic content, and hacker tools sites where an employee can access tools to use for hacking. To be safe, organizations should inform their employees of all the mechanisms they use to monitor them so that the employees can agree to such monitoring or restrictive actions within their job environment that can lead to the exposure of information they would wish to keep private.

# Summary

In this chapter, the essential role of CISOs in HRM has been discussed in great detail. The potential threat from insiders has been highlighted, explaining the need for CISOs to be involved in HRM. The chapter has shown that insider threats are just as risky as external threats and need to be handled with the seriousness with which external threats are handled. The chapter has reiterated a need for a good security posture that is ready to respond to cybersecurity threats.

In the next chapter, we will handle the documentation function of CISO and its importance in a company's security posture and implementation.

# Further reading

Here are some resources that can be used to gain more knowledge on the topics covered in this chapter:

- Security posture: `https://www.balbix.com/insights/what-is-cyber-security-posture/`
- Human error in security breaches: `https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches`
- Preventing insider security threats: `https://searchsecurity.techtarget.com/feature/Ten-ways-to-prevent-insider-security-threats`
- Human error and cybersecurity: `https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html`
- *How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes*: `https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes`
- Human error threats: `https://nevadaitsolutions.com/prevent-human-error-threats/`
- Data breaches: `https://securitybrief.eu/story/more-than-half-of-personal-data-breaches-caused-by-human-error`
- Job listing: `https://www.bmc.com/blogs/it-job-listing/`
- IAM: `https://www.bmc.com/blogs/identity-access-management/`
- *The history of data breaches*: `https://www.erdalozkaya.com/the-history-of-data-breaches/`