CHAPTER 2  
User and Network Infrastructure Planning and Management

**Overview of Chapter and Objective**

This chapter provides readers with a series of steps and tools to improve their organizations’ network infrastructure protection through improved asset access control, awareness and training, data security, protection policies, maintenance procedures, and automated protection processes.

**A**lan, the senior IT engineer for Major Motors, Inc., is spending a relaxing Thursday night at home playing his favorite video game. His company’s TeamTalk remote collaboration tool pops up in his screen’s right-hand corner during the gaming session. That’s weird, he thinks. He had used TeamTalk earlier in the day while working remotely from home. He had used the tool to discuss with his team how they would integrate the networks of the company’s biggest acquisition to date, its former chief parts supplier Acme Motor Manufacturing.

But the meeting ended hours ago. Alan looks at the TeamTalk tool, and no one is there in the meeting room. Maybe he accidentally clicked the TeamTalk icon, he tells himself, and closes the TeamTalk window to return to his game.

When he shows up at the office the following day, everything is in chaos. The company’s manufacturing system has been hacked, and the attackers are systematically erasing the firmware for some assembly line servers. Everyone is running around trying to figure out what to do.

It takes the company all day to recover from what was a sophisticated, baffling attack. Recovering from the attack wasn’t easy because one of the first things the attackers did was erase specific critical backup files. The damage caused by the unknown attackers might have been even worse had not a quick-thinking engineer cut off the power supply to critical servers, which kept damaging malware from propagating across systems.

The FBI and the forensics experts hired by Major Motors spend weeks figuring out what happened. As best they can piece together, a user account with super-user privileges to gain access to every system at the company had logged in and systematically begun scoping out assets before destroying the backup files and erasing the firmware.

However, the investigators can account for all the super-users’ actions, and the log files don’t show any of them logging into the systems. When the investigators tell the company’s chief information security officer Jack about this, he suddenly remembers: Alan had been given temporary super-user privileges for a day to test a few potential new applications a vendor recommended. Alan wasn’t on the latest list of super-users. But that had been weeks ago.

Under questioning by the investigators, Alan swears he did not log into any of the relevant systems at the time of the attacks. Investigators examine Alan’s home computer and find keylogging software that captured Alan’s login credentials for the TeamTalk tool. They are the same credentials Alan used for his temporary super-user access.

The investigators’ report concludes that Alan’s home computer was the conduit through which the attackers gained complete system authorization credentials at the company to wreak havoc.

**I. INTRODUCTION**

As Alan’s situation illustrates, keeping close track of user access to organizational networks can mean the difference between a secure network and a cybersecurity crisis that can subsume your organization. Building safeguards into how you plan and manage your organization’s infrastructure is crucial to ongoing operations and resiliency in the face of a cyberattack. This chapter on User and Network Infrastructure Planning and Management builds on the risk assessment skills developed during the first chapter and delves into the details of how to create and implement security safeguards to protect your organization’s data, systems, assets, and functions. By the end of the chapter, you will know the basic principles of evaluating risks and properly implementing solutions such as patch management, firewalls, back-ups, security awareness, awareness training, and more.

**II. INFRASTRUCTURE PLANNING AND MANAGEMENT IS ALL ABOUT PROTECTION, WHERE THE RUBBER MEETS THE ROAD**

Infrastructure planning and management is all about building safeguards and security controls into your organization’s networks and assets. It’s all about protection. This section will rely heavily on the critical concepts in the Framework for Improving Critical Infrastructure Cybersecurity, developed by NIST, as outlined in [Chapter 1](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml).

NIST developed the Framework to help organizations of all kinds strengthen their cybersecurity practices and, in circumstances where companies are new to cybersecurity, develop and implement those practices. One of the NIST Framework’s most significant components is a series of outcomes or desired secure states that fall under a “Protect” function.

This Protect function:

* supports the ability to reduce the attack surface and limit the impact of an adverse cyber event and
* entails developing and implementing the safeguards needed to minimize risk to critical assets and sensitive information, including access control, patch management, firewalls, back-ups, security awareness, and training.

According to the NIST Framework, protecting your organization involves the following six major cybersecurity categories:

* Access Control
* Awareness and Training
* Data Security
* Information Protection Processes and Procedures
* Maintenance
* Protective Technology

We’ll walk you through each of these essential protection activities in this chapter, offering specific recommendations on how you can get a handle on them. We’ve mapped each recommendation to its specific corresponding NIST Framework subcategory so that you can dig deeper into the growing wealth of resources made available around the NIST Framework.

This chapter will present a general introduction to each of these categories, hitting the high points of what you need to know. We’ll also give you recommended technical standards for each subcategory and suggest that you consult these standards for more details.

As you go through the chapter, bear in mind that there is no one-size-fits-all approach to security controls or developing security policies because each organization is unique. Each organization has its priorities, technical configurations, financial constraints, and operating philosophy. Some recommendations presented in this chapter may not apply to your organization, or may not apply now but might be of use in the future, or may need to be modified and tailored to fit your unique circumstances.

**A. Identity Management, Authentication, and Access Control**

Access control is the first and most crucial step in protecting your organization’s networks and assets. It is simply the process through which your organization ensures that an authenticated user gains access to only what they are authorized to access and nothing else. In the words of the NIST Framework, the outcome of access control is “access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.”

Before we proceed, it’s helpful to make the distinction between authentication and authorization. Authentication is the act or process of determining that a user is who they say they are and gathering information on how they are accessing your systems. For example, Judy in accounting can access the payroll system on the company network using her login ID and password. However, when she tries to access the system from home, she has to provide a second form of authentication by typing in a passcode sent to her phone.

On the other hand, authorization is the act of determining the level of access an authorized user has to systems and data. Judy in accounting is authorized to access the payroll systems but she cannot update software in the network management systems. To effectively implement access control, your organization must first identify which systems need to have controlled access, and under what rules access should be granted.

Determining the systems for which you must control access is entirely contingent on what you deem most valuable or otherwise strategically important. Your risk assessment analysis can be useful in drawing up a list of systems for which access control should be applied and how. In terms of the rules that should apply to the various levels of access, some factors to consider are:

* Connection type
* CRUD enforcement (create, read-only, update, delete)
* Time of day
* Cascading authorization (some authorizations come with obligations for further actions)
* Global permissions
* Combination of privileges

**Voices of Experience  
*On Granting Access***

**Watch Out for Layering Entitlements When Job Functions Change**

*By focusing on the identity and putting the user front and center, you think about the workflows to creating and managing the user’s account. This is the entire user life cycle, often called the “hire to retire” process. Activating and disabling an account is easy. To make sure that there’s segregation of duties, the more difficult part is when the user gets promoted or when the user moves from that accounts payable clerk role to being an accounts payable supervisor. You need to make sure that you are giving them the new rights while removing the old ones. Otherwise, you start layering entitlements on top of them. This can be a big problem, especially for a publicly traded company, especially if you get audits every year and you must comply with Sarbanes–Oxley (SOX)*.

Joe Klein, former CISO, Enersys & BillTrust

Ultimately, the goal of authorization is to employ the principle of “least privilege” necessary to perform job functions. This least privilege rule means that it’s safer and more secure to give users only those privileges they need to complete the tasks covered by their role in the organization. For example, if a user account exists solely to perform back-ups, that account doesn’t also gain the ability to implement software updates.

There are many appropriate steps to implement access control adequately. We’ll go through a few of these in the following sections.

1. **1. Always Be Aware of Who Has Access to Which System, for Which Period of Time, and from Where the Access Is Granted**

(PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.)

Organizations often have to manage many different system account types, from the individual, shared, group, guest, anonymous, developer, or service accounts. Generally speaking, you should restrict accounts by knowledge of passwords. Still, additional measures include restricting by time (temporary), restricting by geography (off-premises access), restricting by source (access control lists), and restricting by certificate (public/private key pairing so that only specific encrypted messages can be accessed).

In the language of the Cybersecurity Council, the objective of this aspect of access control is to “actively manage the life-cycle of system and application accounts, including their creation, use, dormancy, and deletion, and to minimize opportunities for attackers to leverage them.”[**1**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c02.xhtml#c2-note-0003)

To establish access control, it’s essential that your organization accurately tracks and builds into your account activation procedures all of the different system account characteristics mentioned above (and more) that may be specific to your unique circumstances. Ensure that you are consistent with the definition of authorization and users’ access privileges defined for other security controls.

In addition to managing credentials for activating authorization, it’s equally important that your organization establish procedures for \*deactivating\* authorizations, particularly where you set temporary accounts for short-term or emergency purposes. The activation of these temporary accounts often bypasses standard procedures and can get lost in the shuffle if you don’t establish rigorous deactivation processes.

**Relevant Technical Standards for PR.AC-1**

**Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes**

* CIS CSC 1, 5, 15, 16
* COBIT 5 DSS05.04, DSS06.03
* ISA 62443-2-1:2009 4.3.3.5.1
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
* ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3
* NIST SP 800-53 Rev. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

1. **2. Establish, Maintain, and Audit an Active Control List and Process for Who Can Physically Gain Access to Systems**

(PR.AC-2: Physical access to assets is managed and protected.)

Establishing access control procedures is not a helpful activity unless your organization also establishes procedures that prevent unauthorized access, damage, or interference to your organization’s systems. Therefore, it’s crucial to develop a process of verifying who gains physical access to which systems. You can accomplish this process through a variety of means. For example, for gaining access to equipment, the user has to present a card key plus two-factor authentication such as a PIN or a fingerprint.

To maintain adequate physical access to systems, periodic audits of who gained access to which systems are helpful. You will also find it beneficial to keep an access control list containing all of the authorization credentials and the individuals to whom these credentials apply.

**Relevant Technical Standards for PR.AC-2**

**Physical access to assets is managed and protected**

* COBIT 5 DSS01.04, DSS05.05
* ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8
* ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8
* NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8

1. **3. Establish Policies, Procedures, and Controls for Who Has Remote Access to Systems**

(PR.AC-3: Remote access is managed.)

Managing remote access to systems is a crucial part of cybersecurity because the likelihood of unauthorized access increases when remote access to systems is involved. Remote access is simply the act of accessing organizational systems (by individuals or computer processes) through external networks such as the internet.

Your organization should establish formal remote access procedures, policies, and controls for all types of remote communications facilities, including virtual private networks and mobile devices, to determine who has access and what kind of access you give from remote locations.

An important distinction regarding remote access policies and procedures is warranted. In our earlier chapter on risk management, we discussed how you could establish remote access procedures for vendors and other third parties. However, in terms of access control, the remote access policies apply to organizational employees who use their personally owned devices or other privately owned devices in public facilities (such as hotel business centers) to access your systems.

Many organizations handle the problem of remote access by using virtual private networks (VPNs). New evolving solutions replace many VPN solutions using software-defined networking, which focuses on controlling access at the application layer rather than the network layer. A software-defined network can cut down on the complexity of designing and maintaining access control lists. Other methods to protect the organization from threats coming from remote access might include:

* mandatory “health” checks of an employee or other privately owned equipment,
* policy-based access control that assesses the device, the network that the user connects from, and the resources attempting to be accessed, and
* isolation techniques to limit remote access only to sections of the network based on business needs – traditional methods use jump-servers but, as mentioned, evolving solutions offer software-defined networking.

**Relevant Technical Standards for PR.AC-3**

**Remote access is managed**

* CIS CSC 12
* COBIT 5 APO13.01, DSS01.04, DSS05.03
* ISA 62443-2-1:2009 4.3.3.6.6
* ISA 62443-3-3:2013 SR 1.13, SR 2.6
* ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
* NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15

1. **4. Make Sure That Users Have the Least Authority Possible to Perform Their Jobs and Ensure That at Least Two Individuals Are Responsible for a Task**

(PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.)

The least privilege principle states that users should access only the information and resources needed to do their jobs. The principle of separation of duties breaks down tasks so that no single person is in control.

An excellent example of the value of this separation of responsibilities might be the recent rise of spear phishing scams known as business e-mail compromise. These scams, in which the e-mail sender impersonates CEOs and CFOs who are putatively requesting wire transfers, have been targeting treasury and finance departments. The best practice in these situations is to designate the ability to request a wire transfer to one person. Still, approval for the actual funds’ transfer is contingent on another person. This separation would require two people to fall prey to the scam.

Mismanagement of this access control aspect is an excellent way for attackers to access your systems and assets. In one prevalent attacker technique, a privileged user is a victim of a security attack such as malware delivered via phishing. If the user has access to sensitive information assets, the attacker also has access to these assets.

Another common technique is when an attacker uses a process of elimination or guessing to crack a user’s password. The more accounts with access to sensitive assets, the greater the likelihood attackers will gain access to sensitive assets, allowing the miscreants to control the assets.

The following steps can be useful in alleviating these password access issues:

* Develop built-in operating systems that contain lists of accounts.
* Ban users with super privileges from surfing the web or reading e-mail on those accounts.
* Employ a privileged access management system that vaults passwords and offers check-in, check-out of account passwords. Users never know the password until you check them out. After they complete their work, you can change the passwords automatically.
* Enforce strong passwords and strong password protections.
* Implement additional authentication factors for privileged administrative accounts and any externally hosted or available applications on the internet (e.g., cloud, demilitarized zone applications, etc.).
* Limit access to privileged administrative accounts.
* Pro-tip: subscribe to [HaveIBeenPwned.com](http://haveibeenpwned.com/) and establish a process to regularly check to see if any e-mail accounts associated with domains you own show up on the list. Or check the built-in browser password checks that now appear in Chrome or Firefox. Enforce password resets for any accounts that you flag in any of these checks.

**Relevant Technical Standards for PR.AC-4**

**Access permissions are managed, incorporating the principles of least privilege and separation of duties**

* CIS CSC 3, 5, 12, 14, 15, 16, 18
* COBIT 5 DSS05.04
* ISA 62443-2-1:2009 4.3.3.7.3
* ISA 62443-3-3:2013 SR 2.1
* ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
* NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24

1. **5. Implement Network Security Controls on All Internal Communications, Denying Communications among Various Segments Where Necessary**

(PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).)

Network integrity protection deals with network security management, which entails monitoring and implementing security controls on internal networks and communicating with external networks. For example, you can compartmentalize specific network resources, applications, and assets from other groups, and deny access across groups.

Although network segregation is a broad and complex topic outside this chapter’s scope, it boils down to logically grouping network assets, resources, and applications together into compartmentalized areas or segments that don’t trust one another. The benefits of segmenting or grouping assets, aside from improved access control, include:

* greater visibility into network traffic,
* protecting communications as they flow into and out of the organization, and
* setting default-deny policies on all intersegment communications.

For example, employees’ private mobile communications that rely on organizational Wi-Fi connectivity can be segmented so that none of the organization’s systems or data are affected or accessed. Without this segmentation, administrators would be unable to determine how much traffic over the organization’s internet connections are due to employee mobile devices (which pose security risks), much less establish policies barring the private mobile devices from gaining a connection to core system functions.

**Relevant Technical Standards for PR.AC-5**

**Network integrity is protected (e.g., network segregation, network segmentation)**

* CIS CSC 9, 14, 15, 18
* COBIT 5 DSS01.05, DSS05.02
* ISA 62443-2-1:2009 4.3.3.4
* ISA 62443-3-3:2013 SR 3.1, SR 3.8
* ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
* NIST SP 800-53 Rev. 4 AC-4, AC-10, SC-7

**A WORD ABOUT FIREWALLS**

Firewalls are a crucial sub-component of protecting network integrity, and, given the importance of firewalls, we’ll spend a moment discussing them. In general, firewalls are technologies that segment parts of computer systems or networks to block unauthorized access but permit communications outward from the systems or networks. Instead of restricting unauthorized users, firewalls restrict unauthorized communications.

There are numerous types of firewalls and many different vendor products, so the details of how you implement firewalls will vary widely. Regardless of what technology you use or which vendor you select, there are some useful principles to consider when implementing firewalls within your organization:

* Create a policy consistent with your organization’s risk management philosophy that specifies how firewalls should handle inbound and outbound traffic.
* Identify all requirements that you should consider when determining which firewall to implement. Consider how your employees access resources and where the critical assets reside. Is a large population of your employees mobile? Is there heavy adoption of the cloud? It would help if you considered these types of questions because they can affect the solutions you need. If employees are rarely on site and the company uses cloud solutions, an on-premises firewall may not be a good fit.
* Create rule sets that implement the organization’s firewall policy while supporting firewall performance. These rule sets will be dependent on the type of firewall you use and the specific firewall products you deploy.
* Manage firewall architectures, policies, software, and other components throughout the life of the firewall solution. The type of firewall you use can affect the security policies you enforce. If those policies change, you should review the firewall component of your protection strategy. It’s also essential to examine firewall logs and log alerts to identify threats.

You can find more detailed information on installing, managing, and maintaining firewalls in the NIST special publication, *Guidelines on Firewalls and Firewall Policy*, Special Publication 800-41, Revision 1, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>.

1. **6. Associate Activities with a Real Person or a Single Specific Entity**

(PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.)

One of the biggest challenges in identity management is associating a set of online or other digital activities with a specific individual or entity. Although anonymity is helpful in many cases, there are situations where it is crucial to establish an association with a real-life subject reliably.

In these situations, good cybersecurity practice requires what is called identity proofing. In this complex process, you take steps to ensure a user or an entity is who they claim to be to a certain level of certainty. This assurance includes either in-person or online presentation, validation, and verification of the minimum attributes necessary to accomplish identity proofing, such as providing name, address, date of birth, e-mail address, phone number, passport, driver’s license, photos, and even biometric data.

Once you proof an identity, you can bind other authenticated activities to that proof. For example, once a bank proves a customer’s identity to open a checking account, that customer can launch an online payment application bound to the original identifying credentials supplied when opening the account.

**Relevant Technical Standards for PR.AC-6**

**Identities are proofed and bound to credentials and asserted in interactions**

* CIS CSC 16
* COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03
* ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4
* ISA 62443-3-3:2013 SR 1.1, SR 1.2,SR 1.4, SR 1.5, SR 1.9, SR 2.1
* ISO/IEC 27001:2013 A.7.1.1, A.9.2.1
* NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-16,AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3

1. **7. Use Single- or Multi-Factor Authentication Based on the Risk Involved in the Interaction**  
   (PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks.)

As online and digital risks increase in number and grow more complicated, user authentication methods are growing more complex. It’s impossible in the digital era to implement the authentication process with in-person or physical documentation to prove identity for users who want access to critical or sensitive resources.

Single-factor authentication, such as a user ID and password, has proven to be an insecure method for accessing important assets because it is vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, dictionary attacks, shoulder surfing, re-use of credentials stolen in massive data breaches, and many other threats.

On the other hand, multi-factor authentication represents multiple single-factor authentication methods and is generally considered more secure than single-factor authentication. Multi-factor authentication can combine user credentials (IDs and passwords) with mobile phone verification, e-mail verification, PINs, biometric markers such as fingerprints, physical security tokens, or keys such as USB sticks, and other methods.

It will help if you choose whether to deploy single-factor or multi-factor authentication for your systems and assets consistent with your organization’s risk assessment analysis. You should consider giving greater preference to more robust authentication methods for those assets and systems most at risk and most likely to cause damage if malicious actors breach them.

**Relevant Technical Standards for PR.AC-7**

**Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)**

* CIS CSC 1, 12, 15, 16
* COBIT 5 DSS05.04, DSS05.10, DSS06.10
* ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10
* ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
* NIST SP 800-53 Rev. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

**III. AWARENESS AND TRAINING**

Securing and protecting systems and infrastructure requires a lot of skill and training. That’s why one of the chief subcategories in the Protect function of the NIST Framework includes awareness and training guidelines and why one of the top goals of the National Initiative for Cybersecurity Education (NICE), a federal project that began in 2010, is initial and ongoing training for workers in cybersecurity.

As a side note, the increasing use of phishing assessments among all employees is an excellent method to educate and train the workforce about the dangers of phishing e-mails. In essence, your organization might consider sending test phishing e-mails to the workforce and then use the results of those e-mails to educate them on how to spot phishing e-mails.

**Voices of Experience**

***On Awareness and Training***

**Training That Is Most Useful to Employees**

*One of the things we did at Ohio State is we really delved into how do you make advocates of people. One of the big things was this concept of pulling in social influences into your training. We worked with our mobile team to come up a platform which was new and exciting. Small bytes of information about security ideas that we called activities that people could choose to take. First of all we didn’t make it mandatory. We encouraged people to go check the platform out and then we had topics within it*.

**Making Employees Embrace and Connect to Training**

*We have to make it something that would appeal to them personally, so the reality for us was people didn’t care about cybersecurity. But they did care about their own data. They did care about their own banking. They cared about whether their kids were getting bullied online. They cared about privacy of their use of social media, those kinds of things*.

Helen Patton, former Chief Information Security Officer, The Ohio State University

The NIST Framework provides subcategories under the awareness and training category, which all have the same outcome. What we’ll touch on in this chapter is PR.AT-5, which concerns cybersecurity personnel’s understanding of their roles and responsibilities, but in essence the same recommendations apply across all five of the NIST awareness and training subcategories.

**A. Make Sure That Privileged Users and Security Personnel Understand Their Roles and Responsibilities**

(PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.)

You must establish fundamental security skills among select asset users to improve your security posture. This skills development can entail installing or using formal or informal training programs and using standards for determining users’ and personnel’s qualifications.

**Relevant Technical Standards for PR.AT-5**

**Physical and cybersecurity personnel understand their roles and responsibilities**

* CIS CSC 17
* COBIT 5 APO07.03
* ISA 62443-2-1:2009 4.3.2.4.2
* ISO/IEC 27001:2013 A.6.1.1, A.7.2.2
* NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13

**IV. DATA SECURITY**

Nothing is more valuable to an organization’s functioning than the data it maintains, which is why hackers seek out databases and other sources of data to steal from business, government, and non-profit organizations. Data security is simply the policies and procedures for protecting data when transmitted or “in transit” and when it’s “at rest” or in storage. The NIST Framework defines data security as “information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.”

In short, any effective security program must protect the value and integrity of your organization’s data. The data protection steps we’ll touch on in this section of the chapter should go a long way to ensuring that your data – both in transit and at rest – is protected.

Before we begin, we should note that many organizations’ data are accessible through database management systems (DBMS), which require managerial, technical, and physical controls consistent with the organization’s risk assessment strategy.

**A. Protect the Integrity of Active and Archived Databases**

(PR.DS-1: Data-at-rest is protected.)

All organizations should institute mechanisms that address the security, integrity, and confidentiality of information in active and archived databases. The integrity of data means that the data is complete without any alteration from its original state.

No single control can ultimately ensure your data integrity, but various techniques can help protect it. You can maintain the integrity of your databases by implementing several techniques, such as:

* Cryptography
* File-share scanning
* WORM (write once, read many discs that prevent erasure or alteration of data)
* Maintaining databases offsite and not online

Before implementing methods to protect your databases, it’s helpful to identify and address potential sources of damage to data to select the best approach. In particular, users should familiarize themselves with the unique needs of protecting the vast amount of media stored in databases, often precious and copyrighted material, to ensure that the content cannot be accessed or altered.

Finally, if your organization chooses to use third-party off-site storage vendors, make sure to examine their security policies so that you can have the comfort of knowing that those policies are adequate for your needs.

**Relevant Technical Standards for PR.DS-1**

**Data-at-rest is protected**

* CIS CSC 13, 14
* COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
* ISA 62443-3-3:2013 SR 3.4, SR 4.1
* ISO/IEC 27001:2013 A.8.2.3
* NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28

**B. Protect the Confidentiality and Integrity of Corporate Data Once It Leaves Internal Networks**

(PR.DS-2: Data-in-transit is protected.)

Communication between internal and external networks, also called data-in-transit, must be protected from unauthorized parties, including malicious hackers, through any one of several means, including encryption or using separate secure systems. Because communications are continually flowing into and out of a wide range of devices, including servers, mobile devices, tablets, printers, network-connected copiers, scanners, fax machines, and dozens of other devices, ensure your data protection plans encompass all of these forms of communications devices.

Besides the dozens of other specific devices that you should incorporate into data-in-transit security plans, you should think about data movement from an assortment of industry-specific devices and machines to more endpoints. Many of these endpoints, particularly many vendor endpoints, do not offer acceptable encryption practices, such as HTTPS protection. It would help if you considered treating any data that flows through to endpoints that use bad encryption practices as confidential and take whatever steps necessary to protect the data.

Generally, when working with outside communications network providers that don’t meet your security requirements, you should consider implementing compensating security controls to cover the deficiency.

**Relevant Technical Standards for PR.DS-2**

**Data-in-transit is protected**

* CIS CSC 13, 14
* COBIT 5 APO01.06, DSS05.02, DSS06.06
* ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2
* ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
* NIST SP 800-53 Rev. 4 SC-8, SC-11, SC-12

**C. Assure That Information Can Only Be Accessed by Those Authorized to Do So and Protect Hardware and Storage Media**

(PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.)

From the perspective of data and network security, we can define integrity as the assurance that information can only be accessed or modified by those authorized to do so. By maintaining strict authorization procedures, organizations can protect data integrity by making administrative functions of servers accessible only to network administrators.

Among the steps you can take in maintaining strict authorization procedures are:

* Restrict data access by implementing controls that make administrative functions on the server available only to administrators.
* Document all authorized users by level.
* Document admin procedures and maintenance activities.
* Consider file integrating monitoring solutions for critical information assets, particularly those stored in unsecured file shares, given the prevalence of network-propagating ransomware.

Moreover, physical protection is also key to data and network integrity. To keep assets physically protected, take steps to protect them from damage or interference. These steps can include keeping transmission media (such as cables and connectors) covered and protected to ensure that bad actors can’t tap them and protecting hardware and storage media from power surges, electrostatic discharges, and magnetism.

**Relevant Technical Standards for PR.DS-6**

**Integrity checking mechanisms are used to verify software, firmware, and information integrity**

* CIS CSC 2, 3
* COBIT 5 APO01.06, BAI06.01, DSS06.02
* ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8
* ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
* NIST SP 800-53 Rev. 4 SC-16, SI-7

**D. Keep Your Development and Testing Environments Separate from Your Production Environment**

(PR.DS-7: The development and testing environment(s) are separate from the production.)

Anyone who has ever developed a software system or even a website has learned this subcategory of the NIST Framework the hard way. Development and testing of new techniques, software, or web interfaces should always occur away from the production environment because development or testing systems might contain bugs that can wreck production systems’ memory, CPUs, and content.

Suppose you introduce a faulty development or test system to the production environment. In that case, you risk damaging your organization’s reputation and revenues, not to mention disrupting many personnel who have to deal with the problem. Depending on the damage caused by creating a development or test system in the production environment, you might have to spend substantial sums hiring contractors to do the clean-up.

Conducting development work or test work on production systems are two different activities. Development work allows developers to make changes and test out new options that they might not have been introduced into the production environment before. Developers often use integrated development environments that consist of various development tools such as Microsoft Visual Studio and other tools for logging or debugging.

Testing is identical to the production environment and could be a way for developers to test out updated software or enhance applications present in the production environment. Developers can install several different testing environments depending on the objectives pursued. Sometimes they want to test the performance of various parts of the production system. Sometimes they test the security hardiness of the production environment.

The bottom line is that to minimize the risk of business disruption, you should conduct both development and testing on systems separated from the production environment.

For further technical information on how best to separate development and test from the production environment, NIST has mapped this subcategory to the following standards:

**Relevant Technical Standards for PR.DS-7**

**The development and testing environments(s) are separate from the production**

* CIS CSC 18, 20
* COBIT 5 BAI03.08, BAI07.04
* ISO/IEC 27001:2013 A.12.1.4
* NIST SP 800-53 Rev. 4 CM-2

**E. Implement Checking Mechanisms to Verify Hardware Integrity**

(PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.)

Ensuring the accuracy and integrity of hardware components in your systems is crucial to your organization’s security. Therefore, it’s helpful to implement checking mechanisms that periodically verify the integrity of the hardware.

Independent testing authorities can conduct this verification process, or you can run the checking mechanisms in-house. Either way, the following are just some considerations to bear in mind when conducting hardware verification tests:

* Test your hardware under conditions that simulate their expected real-life situations, including storage, operations, and maintenance environments.
* Ensure that the hardware conforms with local environmental requirements, including shelter, space, furnishings and fittings, electrical power supply, and relevant extremes of temperature, humidity, and pollution.
* Ensure that you have complete and appropriate documentation for the hardware.
* Verify that the hardware operates normally under abnormal conditions.

**Relevant Technical Standards for PR.DS-8**

**Integrity checking mechanisms are used to verify hardware integrity**

* COBIT 5 BAI03.05
* ISA 62443-2-1:2009 4.3.4.4.4
* ISO/IEC 27001:2013 A.11.2.4
* NIST SP 800-53 Rev. 4 SA-10, SI-7

**V. INFORMATION PROTECTION PROCESSES AND PROCEDURES**

You should ideally develop all your information security programs according to processes, policies, and procedures. To be most effective, you should ensure that policies emanate from the organization’s top level. In addition to policies that apply to top-level employees, including security personnel, you should establish specific guidelines for all workforce members, including staff, vendors, volunteers, and just about everybody in the organization. These policies should have procedures and expectations for workers to follow.

The NIST Framework puts it this way: “Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.”

In this next section, we’ll walk through some of the tasks needed to develop security program processes, procedures, and policies.

**A. Create a Baseline of IT and OT Systems**

*(PR.IP-1 A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g., concept of least functionality).)*

This subcategory’s primary purpose is to foster an environment where organizations adopt baseline configurations of their IT and OT systems, keeping in mind some bedrock cybersecurity principles discussed later in the chapter, least privilege and least functionality. “Baseline configurations are documented, formally reviewed, and agreed-upon sets of specifications for information systems or configurations items within those systems.”[**2**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c02.xhtml#c2-note-0004)

Baseline configurations serve as the basis for all future changes to the systems and are the most stable version. They can include “information about information system components (e.g., standard software packages installed on work computers, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.”

In some contexts, baseline configurations serve to lay down the markers for permitted or prohibited processes. The bottom-line goal is to create a secure environment that the organization alters only after deliberation and consideration of the security principles that underpin that environment.

For more information on the topic of baseline configurations, NIST has mapped the following standards to this subcategory:

**Relevant Technical Standards for PR.IP-1**

**A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)**

* CIS CSC 3, 9, 11
* COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
* ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
* ISA 62443-3-3:2013 SR 7.6
* ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
* NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

**B. Manage System Configuration Changes in a Careful, Methodical Way**

*(PR.IP-3: Configuration change control processes are in place.)*

This task is part of a much broader subject known as configuration management, a vast and complex discipline far more expansive than this chapter’s scope. We’ll spend some time boiling down critical aspects of configuration management that should be helpful to you, even if your organization doesn’t have the resources to embrace many aspects of configuration management fully.

Configuration management is a technique for monitoring and controlling all forms of development activity. To monitor and control development activity, you should construct the system’s basic structure through some sort of identification scheme. You should also put a management system into place to designate the organization’s management level needed to make changes at various scheme layers.

Configuration management spells out the methods for controlling changes to assets throughout the assets’ life cycles. Using a life-cycle process provides control over an organization’s assets, which has several strategic security benefits, including:

* maintaining the integrity of system configurations so that you can make rational changes in an orderly way,
* keeping top management plugged in, and
* providing a basis for measurement.

You should assign each role in the configuration management process to one of three appropriate managers. First, a configuration manager should be designated who makes sure that each requirement of change management is carried out.

It’s also helpful to designate a “baseline” manager to track changes in a change management ledger (CML) and maintain all products’ libraries or records. The baseline manager ensures that all configuration items (CIs) in the product configuration management plan are accounted for and maintained according to a specified identification scheme.

Finally, a verification manager helps ensure that product integrity is maintained during the change process. The verification manager also maintains documentation of the change process and other vital tasks.

For any of these managers to perform their tasks, you should develop a configuration management scheme to establish the baseline. You should maintain the scheme throughout the life cycle of the asset. Each asset should have a product identification number in the scheme for easy reference and tracking.

Once you establish the baseline, good practice suggests that you make any changes to the baseline at the highest management level possible. For some organizations, this can be a complex and challenging task requiring management input at the top ranks. Once you build baseline configurations for critical assets, it’s helpful to scan for changes to the baseline periodically.

And a final note: acceptable CI management practices call for:

* Only open ports/protocols necessary for devices to function.
* ALWAYS change default administrative account passwords.
* Deploy “switch user” functionality to access root accounts, such as sudo. This functionality means that higher priority users can gain control over lower priority users.

**Relevant Technical Standards for PR.IP-3**

**Configuration change control processes are in place**

* CIS CSC 3, 11
* COBIT 5 BAI01.06, BAI06.01
* ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3
* ISA 62443-3-3:2013 SR 7.6
* ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
* NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

**A WORD ABOUT PATCH MANAGEMENT**

One crucial activity that falls under configuration management that we highlight is patch management or incorporating vendor software and firmware patches in a reasonable, risk-aware, and secure manner. Many recent high-profile security failures, most prominently that of credit rating agency Equifax, were due to failed patch management, which in turn was due to poor organizational configuration management practices and policies.

Although it might seem like vendor patches should be implemented immediately, patching system assets should proceed consistently and orderly as all system changes under your organization’s configuration management policies. Consistent with your organization’s risk management plan, you should develop a risk assessment process to evaluate vendor-released patches’ criticality and applicability. This risk assessment should balance the potential downsides or risks of not patching the reported vulnerability against the extent of downtime and impaired functionality, and possible loss of data while you implement patches.

Keeping track of newly issued patches and conducting patch risk assessments can be an overwhelming task, particularly for an organization that uses a wide range of IT- and OT-specific technologies. Depending on your organization’s size and complexity, it might be helpful to use an automated tool and maintain a database of monitored systems to evaluate which patches are critical, which ones are useful, and which ones are not needed. NIST has a guide to help steer you through the creation or adoption of automated patch management technologies: SP 800-40 Rev. 3, *Guide to Enterprise Patch Management Technologies* at <https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final>.

**C. Perform Frequent Backups and Test Your Backup Systems Often**

*(PR.IP-4: Backups of information are conducted, maintained, and tested.)*

Because the information in your databases is valuable and because all systems are prone to failure, maintaining up-to-date backups of databases and other important information is critical to resiliency in the event of a security attack, equipment failure, or human error. A backup is simply a copy of information from your systems to another device for recovery or archiving.

In the event of a failure or attack, important information can be copied from the backup media into your production system in a process called data restoration. The following suggestions ensure that your backup plan will be available in those cases where you need to perform a data restoration:

* Implement a system for periodically checking to ensure that backups are taking place properly.
* Ensure the backup system receives the same protection level as the original data based on its value.
* Keep ongoing accurate records of how you perform backups.
* Keep backups in off-site storage away from the original systems, so they are not subject to the same damage of failure or attacks. (Make sure the facility meets your security standards!) This distance is significant in incidents that involve ransomware attacks.

**Relevant Technical Standards for PR.IP-4**

**Backups of information are conducted, maintained, and tested**

* CIS CSC 10
* COBIT 5 APO13.01, DSS01.01, DSS04.07
* ISA 62443-2-1:2009 4.3.4.3.9
* ISA 62443-3-3:2013 SR 7.3, SR 7.4
* ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
* NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

**D. Create a Plan That Focuses on Ensuring That Assets and Personnel Will Be Able to Continue to Function in the Event of a Crippling Attack or Disaster**

*(PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.)*

Response plans and disaster recovery plans are at the core of cybersecurity preparedness. Response plans, more often referred to as business continuity plans, are the crux of preserving organizational resiliency during extreme crises.

The flip side of response plans or business continuity plans is disaster recovery, and the two are often referred to as one concept – business continuity/disaster recovery. Disaster recovery is simply the process after which an organization resumes functioning after a disaster.

You should develop business continuity/disaster recovery plans to ensure that personnel and assets are available, protected, and able to function during and after extreme situations. The details of these plans are dependent on the organization’s activities, but some factors to consider are:

1. How employees will communicate.
2. Where employees will go.
3. How to keep core functions operational in the event of a severe attack.

**Relevant Technical Standards for PR.IP-9**

**Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**

* CIS CSC 19
* COBIT 5 APO12.06, DSS04.03
* ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1
* ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
* NIST SP 800-53 Rev. 4 CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17

**VI. MAINTENANCE**

The development and documentation of system maintenance procedures and policies are critical to protecting your organization’s ongoing operations. There are no blueprints for these policies and procedures, which can vary widely. But it is essential to develop a formal, documented information system maintenance policy that aligns with the policies your organization has established. At the same time, it’s necessary to keep the maintenance policy updated with any changes in your system’s IT or security maintenance programs.

Maintenance of assets encompasses all types of care for all kinds of components, not just IT assets, including:

* system software and business applications,
* network devices including scanners, copiers, printers, and voice-activated machines, and
* OT-specific software and devices.

For all of these organizational assets (and more), it’s critical to establish who is responsible for maintenance, maintenance tools, and remote assets.

In this section of the chapter, we’ll talk about how to perform maintenance tasks and repairs promptly and how to manage maintenance and diagnostic activities for third parties upon which your organization relies.

**A. Perform Maintenance and Repair of Assets and Log Activities Promptly**

*(PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools.)*

The primary way to perform maintenance and repair of assets promptly is to ensure your organization schedules, performs, documents, and reviews records of maintenance and repairs on all system components based on what manufacturers or vendors define in their specifications, as well as your organizational requirements.

To achieve optimal maintenance, you should consider the following factors:

* Ensure your organization is in charge of all maintenance procedures, whether they are performed on site or remotely.
* Designate an employee who explicitly authorizes the removal of systems or system assets for off-site maintenance and repairs.
* Inspect and sanitize all media that are removed off site for repairs.
* When making repairs, check for all potentially impacted security controls to ensure they are still fully operational after performing maintenance and repairs.
* Establish a process for authorizing maintenance and repair personnel.
* Maintain a list of third-party personnel and maintenance organizations.

**Relevant Technical Standards for PR.MA-1**

**Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools**

* COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05
* ISA 62443-2-1:2009 4.3.3.3.7
* ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6
* NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5, MA-6

**B. Develop Criteria for Authorizing, Monitoring, and Controlling All Maintenance and Diagnostic Activities for Third Parties**

*(PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.)*

It is widespread for many organizations to outsource maintenance and repair to third-party vendors. If your organization uses third parties for maintenance and repair procedures, ensure that the maintenance policy spells out criteria for authorizing, monitoring, and controlling all maintenance activities. These activities should be consistent with your organization’s policies.

**Voices of Experience**

***On Removable Media***

**Overlook Removable Media at Your Own Peril**

*Removable media are often overlooked as a risk. When you look at awareness and training around phishing attempts by adversaries, you will hear countless stories about the conference attendee that goes to a booth and picks up a flash drive in a fishbowl or they will find a flash drive on the ground walking into their office. They simply plug it into their computer. There are so many times that a ransomware or a type of commodity malware was executed just by plugging in that flash drive. It is basic, but locking that down is still a highly effective control*.

Joe Klein, former CISO, Enersys & BillTrust

**Relevant Technical Standards for PR.MA-2**

**Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access**

* CIS CSC 3, 5
* COBIT 5 DSS05.04
* ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8
* ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1
* NIST SP 800-53 Rev. 4 MA-4

**VII. PROTECTIVE TECHNOLOGY**

This element of protecting your organization’s assets deals with defining controls for protection settings that technical mechanisms can implement, often referred to as technical security architecture. In the parlance of the NIST Cybersecurity Framework, “Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.”

**A. Restrict the Use of Certain Types of Media On Your Systems**

*(PR.PT-2: Removable media is protected and its use restricted according to policy.)*

Computerized media (as opposed to non-computerized media such as paper) are often used to knowingly or innocently inject malware into virtually every kind of system. It is helpful to restrict the use of specific devices on your plans.

Among the devices for which you might want to draw up restrictions are:

* diskettes
* magnetic tapes
* external or removable hard drives
* flash drives
* compact discs
* smartphones
* tablets
* laptops
* organization-specific mobile or removable gear

**Relevant Technical Standards for PR.PT-2**

**Removable media is protected and its use restricted according to policy**

* CIS CSC 8, 13
* COBIT 5 APO13.01, DSS05.02, DSS05.06
* ISA 62443-3-3:2013 SR 2.3
* ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
* NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8

**B. Wherever Possible, Limit Functionality to a Single Function Per Device (Least Functionality)**

(PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.)

**Voices of Experience**

***On Least Functionality***

**Turn on Only Those Services Needed**

*The principle of least functionality relates to the computers themselves. Here you should only be turning on the services, opening ports, and installing the software that is needed. One organization where I was a cybersecurity executive when I first came in, I asked about the images that they used and was told they were provided by Microsoft with the default installation of Windows 7. My response was “no”. When you install Windows, the default functionality is excessive. Look toward the available hardening guides to start with a basic build then turn components on afterwards. Turning on a service is quite easy. Having a live server that is used in production and hardening it after the fact is extremely painful*.

Joe Klein, former CISO, Enersys & BillTrust

Many system components can serve multiple functions, but the principle of least functionality, whereby a device serves a single process (for example, a server can be an e-mail server or a web server but not both combined), can help you better manage authorized privileges to the services the device supports. Moreover, offering multiple services over a single device increases risk.

If you do offer multiple services over a single device, it is helpful to conduct periodic reviews to determine which services you can eliminate from the device. Finally, removing unnecessary ports or protocols can help maximize the least functionality status of your devices.

**Relevant Technical Standards for PR.PT-3**

**The principle of least functionality is incorporated by configuring systems to provide only essential capabilities**

* CIS CSC 3, 11, 14
* COBIT 5 DSS05.02, DSS05.05, DSS06.06
* ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
* ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
* ISO/IEC 27001:2013 A.9.1.2
* NIST SP 800-53 Rev. 4 AC-3, CM-7

**C. Implement Mechanisms to Achieve Resilience on Shared Infrastructure**

*(PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.)*

Resilience is critical to coping with incidents that could impede your operations, from minor incidents to catastrophic events. Achieving resilience is a significant effort that results from extensive planning for a host of activities, including prevention, protection, response, and recovery efforts.

Because modern technology networks typically serve as shared infrastructure initially designed for a limited set of services but are increasingly adapted to run multiple services not envisioned originally, you should develop and implement mechanisms so that failure of individual services don’t cascade to cause failures among other services.

Among the mechanisms that you can implement to help achieve resilience requirements in every day and adverse situations are:

* **Fail-safe**: Fail-safe is an engineering concept holding that in situations with composite components, such as shared infrastructure, you should design the composite so that the parts fail in a “safe” way not to bring down the entire infrastructure.
* **Load Balancing**: Load balancing is a technique that distributes workloads across multiple computing resources such as computers, disk drives, CPUs, and other assets to optimize resource use, minimize response time, increase availability of applications, and prevent overloading any computing resource. Load balancing has traditionally been accomplished with hardware appliances but increasingly is achieved with software-defined technology.
* **Hot-Swap**: A hot swap is replacing a system component, whether a computer, a hard drive or even a power supply, while the system using it continues its operations.

**Relevant Technical Standards for PR.PT-5**

**Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations**

* COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
* ISA 62443-2-1:2009 4.3.2.5.2
* ISA 62443-3-3:2013 SR 7.1, SR 7.2
* ISO/IEC 27001:2013 A.17.1.2, A.17.2.1
* NIST SP 800-53 Rev. 4 CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

**SUMMARY**

Here are some of the central lessons about user and network infrastructure planning and management that we’ve learned from this chapter:

* Access control, which ensures that a user is who they say they are (authenticated) and has access to only what they should access (authorized), is the first step in protecting an organization’s systems and assets.
* Restrict user account access by several crucial factors, including time (permanent or temporary), geography (in-house versus external), type of content (confidential versus non-confidential), and other factors that shape your organization.
* Develop a process of who should gain physical access to systems.
* Establish formal remote access procedures, policies, and controls for all types of remote communications facilities.
* Follow the principle of least privilege and separation of duties, with users having access to only those resources they need to do their jobs and break down tasks so that a single person is in control.
* Protect your organization through network segmentation, grouping network resources, applications, and assets into specific groups.
* Use identity proofing to be certain that individuals are who they say they are and then bind authenticated activities to that proof.
* Consider multi-factor authentication for assets and systems most at risk.
* Ensure that users understand their roles and responsibilities through awareness training.
* Choose from several different methods to protect data-at-rest and data-in-transit.
* Use integrity checking mechanisms so that information can only be accessed or modified by those authorized to do so.
* Make sure your development and testing mechanisms are kept separate from your production environment.
* Implement checking mechanisms that periodically verify the integrity of your hardware.
* Create a baseline of systems that reverts to known secure versions and manage configuration changes in a careful, systematic way.
* Perform frequent back-ups, test your backup systems often and keep your backup systems off site.
* Create plans for personnel to function in the event of an attack.
* Perform maintenance of assets and log activities.
* Develop criteria for authorizing, monitoring, and controlling all maintenance activities of third parties.
* Restrict certain types of media use (e.g., thumb drive) on your network.
* Limit functionality to a single use per device.
* Develop and implement mechanisms so that failure of individual services don’t cascade to cause failures among other services.

**CHAPTER QUIZ**

Now we’re going to give you a short quiz that tests what you learned in the chapter using the scenario we presented initially. You can find the answers at the end of the book.

1. **1. Which of the following made Major Motors’ recovery from the attack take longer than it should have? (Select One)**
   1. **a.** The company’s databases were not adequately protected.
   2. **b.** The company didn’t use firewalls, or the hackers wouldn’t have gained access to assets.
   3. **c.** The company didn’t maintain at least some of its critical backup databases off site.
2. **2. Which two essential steps in managing authorization credentials did the company miss?**
   1. **a.** The company failed to establish formal remote access procedures.
   2. **b.** The company failed to maintain an up-to-date access control list that contains all of the authorization credentials and the individuals to whom these credentials apply.
   3. **c.** The company failed to deauthorize Alan’s temporary super-user account when it was no longer needed.
3. **3. Which of the following protective principles could have averted the company's disaster altogether?**
   1. **a.** The principle of least functionality.
   2. **b.** The principle of least privilege.
4. **4. Which of the following access control policies *might* have averted hackers from attaining access to Alan's credentials? (Select One)**
   1. **a.** The company should have required Alan to use a VPN even while he was playing his video game.
   2. **b.** The company should have conducted a “health check” on Alan’s computer if he had permission to work remotely using it.
   3. **c.** The company should have segmented the network so that Alan couldn't access anything from his home computer.

**ESSENTIAL READING ON NETWORK MANAGEMENT**

Ciprian Rusen, User Accounts, Groups, Permissions and Their Role in Sharing, *How-to-Geek*, Updated April 30, 2019, at <https://www.howtogeek.com/school/windows-network-sharing/lesson1>.

Nicolas Mayer and Jocelyn Aubert, A Risk Management Framework for Security and Integrity of Networks and Services, *Journal of Risk Research*, June 24, 2020, at <https://www.tandfonline.com/doi/full/10.1080/13669877.2020.1779786>.

Jessica Dawson and Robert Tomson, The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance, *Frontiers in Psychology*, June 12, 2018, at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6005833>.

**Notes**

1. [**1**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c02.xhtml#rc2-note-0003) CIS Security, Asset Monitoring and Control, [https://www.cisecurity.org](https://www.cisecurity.org/)/controls/account-monitoring-and-control/#:~:text=CIS%20Control%2016This%20is%20a,for%20attackers%20to%20leverage%20them.
2. [**2**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c02.xhtml#rc2-note-0004) NIST, NIST Special Publication 800-53 (Rev. 4) at <https://nvd.nist.gov/800-53/Rev4/control/>CM-2#:~:text=Baseline%20configurations%20are%20documented%2C%20formally,or%20changes%20to%20information%20systems.