CHAPTER 1
Cybersecurity Risk Planning and Management

**Overview of Chapter and Objective**

This chapter is the most foundational section of the book because it discusses how to establish knowledge of the systems in place and how to inform management of those systems’ risk profiles. It also discusses how to develop plans for dealing with the highest priority risks. The goal is to help the reader develop an understanding necessary to manage cybersecurity risk to systems, assets, data, and capabilities.

**J**ohnson Transportation is one of the world’s largest shipping companies. Joanna, the director of network management inside the company’s IT department, is walking toward the office kitchen to get a cup of afternoon coffee when she passes a colleague’s office.

Out of the corner of her eye, she sees that the screen on his desk suddenly goes dark.

As she walks past another colleague’s desk, another screen goes dark. She keeps walking and sees that screens are blacking out as far as she can see. She wonders if there has been a power failure in the server room, which has twice shut down systems suddenly. She heads back to her desk.

Her phone is ringing, and a junior IT engineer is sitting in her office. She has a growing sense of dread that something is really, fundamentally wrong. Tom, the company’s CIO, calls her to ask if she has any information on the computer blackouts. Joanna tells him she has no idea what happened or where the problem originated.

She checks with John, the head of IT, who is as mystified as she is about the blackout. Some systems, such as voice communications, shipping management, and personnel, never fully went down. They flickered briefly but are now operating normally. Something seems to be wrong with only some routers, although it’s tough to tell which ones.

Joanna is now frantic. Which routers are causing the problem, and where are they? Now that she thinks of it, an IT consultant installed new routers last week. Could they be the cause of the problem? Joanna digs through her inbox to find the consultant’s paperwork on those installations. Everything has been so crazy she hasn’t had time to focus on the new equipment. As her phone lines continue to ring, people are pouring into her office, wanting answers.

She calls everyone who might know what happened. After 45 minutes, she’s no closer to figuring out where the possibly faulty routers are or even if they’re the cause of the problem. Suddenly the company CEO, Nils, is at her office door. What’s going on? All the booking systems are down – in the shipping business, booking systems control everything – and he wants to know what’s going on. He asks her: “Could this be a cyberattack?”

**INTRODUCTION**

As Joanna’s nightmare illustrates, digital security emergencies can encompass entire organizations and destroy customer relationships. If Joanna is well-prepared to manage risks, she can handle this urgent scenario so that Johnson Shipping incurs as little damage as possible.

Cybersecurity risk planning and management is the first step toward helping your enterprise follow a path toward digital security and safety. Still, it can sometimes look daunting to non-cybersecurity professionals. Just know that the first step toward managing a cyber incident is to plan for it in advance.

This book will walk you through how to establish helpful knowledge of information technology and operational technology systems you have in place and develop plans for dealing with the highest priority risks. If you follow the practical advice outlined here, you should have the necessary knowledge to begin managing cybersecurity risks to your organization’s systems, assets, data, and capabilities.

**I.  WHAT IS CYBERSECURITY RISK MANAGEMENT?**

One of the critical foundations of a secure organization is to develop a solid practice of cybersecurity risk management. What is cybersecurity risk management?

Cybersecurity risk management is simply looking at what could go wrong and then coming up with ways to minimize those problems. It’s basically what most of us try to do daily to ensure things go as smoothly as possible in our lives, whether organizing our time, managing our finances, or watching over our children’s lives.

In the same way, cybersecurity risk management is coming up with ways to make sure things go as smoothly as possible with our IT- and OT-related and mission-specific assets. As is true with our everyday lives, managing cybersecurity risks is an ongoing, multi-dimensional process.

One significant distinction exists with cybersecurity that doesn’t always apply in our daily lives: within an organization, everyone needs to be involved in managing cybersecurity risks, from the top level of decision-makers down to the employees responsible for putting into practice the policies that decision-makers establish.

As is true in our day-to-day lives, risk management in cybersecurity can be complicated and daunting, with endless topics to explore. But what we’ll cover in this chapter hits some fundamental practices and activities that should hold you in good stead as your steer your organization on the road to sound and effective cybersecurity.

**A.  Risk Management Is a Process**

Before we jump into actual risk planning and management practices, a bit of the necessary background is in order. In addition to the cybersecurity framework discussed in the Preface, the National Institute of Standards and Technology (NIST) has also developed a cybersecurity risk management framework that characterizes the concept as a comprehensive process that requires organizations to:

1. **1. Frame risk** – Determine how much risk your organization is willing to take on given constraints and upper management goals.
2. **2. Assess risk** – Determine the importance of various assets, know which are protected, and the degree to which the assets are vulnerable.
3. **3. Respond to Risk Once Determined** – Come up with plans of action if the risks turn into adverse realities.
4. **4. Monitor Risk on an Ongoing Basis** – Check risk plans to ensure you have implemented them and updated them as situations change based on ongoing or periodic monitoring of those plans.

Even though cybersecurity risk management should be a part of everybody’s job in an organization, it’s crucial to establish clear roles of responsibility within your organization of who will be held accountable for the risks you face or who will “own” the risks you face, as we discuss later in the chapter. Although this job has typically fallen on the organization’s chief information security officer (CISO) or comparable IT executive, some cybersecurity experts are increasingly recommending that the ownership of risk should fall on the executives who have to cover costs if the threat materializes.

This notion of assigning ownership based on materialized risk losses may not fit your organization or business model. But the point is to establish clarity of risk responsibility and roles throughout your organization. Otherwise, some or even many risks may fall through the cracks of diffused responsibility, and you may never address them adequately until it’s too late.

The next section will walk you through some of these components of cybersecurity risk management. Specifically, we will introduce you to key concepts in the NIST cybersecurity framework, as discussed in the Preface.

**II.  ASSET MANAGEMENT**

When it comes to asset management, most people first think about a crucial cybersecurity element, commonly called “security hygiene.” On a day-to-day basis, all IT and OT assets must be appropriately managed and kept in as secure a manner as possible.

Among the top tasks in this practice of good cybersecurity hygiene, you should:

* patch software as soon as vendor security updates are issued, unless your patch management approach suggests otherwise,
* protect all relevant systems with up-to-date antivirus protection, and
* secure all assets through access controls, including authentication (strong passwords, multi-factor for critical systems externally accessible) and authorization (role-based access control or least privilege).

Fundamentally, at the core of any cybersecurity risk assessment or management program is knowing what assets you have, keeping track of them, and making sure you know which assets employees, vendors, and others have permission to use. In the NIST Framework’s parlance, most functions that qualify as asset management fall under the core function of “Identify.”

All asset management efforts first require identifying those assets to lay a foundation for managing risks to those assets. It is almost impossible to protect systems and software – and your organization – without first developing a process to identify those systems and software.

**Voices of Experience
*On Asset Management***

**If you don’t know what you have, you don’t know what you need to protect**

*The most fundamental thing that organizations should be doing is asset management. If you don’t know what you have, you don’t know what you need to protect or how to protect it or what change management looks like or what a supply chain looks like. There are so many things that stem from simply knowing and managing what you have*.

*Most business don’t want to spend the time, money, or effort to manage their assets that way. If I manage my most critical stuff at least kind of well, I’m probably doing enough to not hemorrhage money or go out of business*.

*The key challenge for them is to understand what’s critical*.

*I work with a lot of boards and executives. It’s basically their jobs to take as much risk as they can. It’s not to take as little risk as they can. In fact, it’s exactly the opposite. So, you’re looking at the leadership of the organization, in almost every case is driving as fast and as hard as they can to take as much risk as they possibly can. The risk management side of the house is looking at it from exactly the opposite perspective*.

Patrick Miller, founder of the Energy Sector Security Consortium and U.S. Coordinator for the Industrial Cybersecurity Center

The NIST Framework defines the outcome or goal of asset management as the “data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.”

The set of processes that make up asset management are designed to manage the life cycle and inventory of technology assets providing value to organizations by:

* lowering IT and OT costs,
* reducing IT and OT risk,
* improving productivity through proper and predefined asset management,
* maximizing the value of the organization’s assets, and
* increasing knowledge of who in the organization needs what kinds of assets.

In this section, we’ll review some of the critical aspects of asset management that you should know to keep your operations as secure and reliable as possible.

**A.  Inventory Every Physical Device and System You Have and Keep the Inventory Updated**

This recommendation closely aligns with a critical subcategory of the NIST Framework, which is “ID.AM-1: Physical devices and systems within the organization are inventoried.” We recommend you learn more about this subcategory and all the NIST subcategories we reference throughout the book.

We’ll provide some helpful technical standard and informative reference resources at the end of each section that NIST has mapped to its Framework.

One of the most important and yet least practiced cybersecurity tasks conducted worldwide is to conduct asset inventories and keep them updated. You cannot defend what you don’t know exists.

This critical task should extend to your headquarters or remote locations, whether that’s a local Starbucks or a home office in Kansas City. You can create an up-to-date inventory of all assets that store or process information on a simple spreadsheet for smaller organizations or within a configuration management database (CMDB) for large organizations. The critical requirement is that an inventory is kept and maintained. Many organizations fail on this crucial security activity because they do not know where to start.

One straightforward approach is to gather your team to just whiteboard a list of systems types. For example:

*End-user device*

* laptops
* phones

*Servers*

* virtual
* physical

*Cloud platform*

* SaaS
* PaaS
* IaaS

**Voices of Experience
*On Asset Management***

**Work from Home Environments Raise the Stakes on Asset Management**

*One of the things that we did as we established a single source of truth is we combined the asset management details with the HR records and what were one of the things that we started watching for was if people were shipping back their laptops shortly after they’re no longer with the company. That’s something that we wanted to automate because we’re such a distributed workforce in the post pandemic work from home kind of environment. You know you don’t want to have something that requires them to go physically to IT and IT to manually record the status. You want to put the data to work. So this asset management data can be combined with HR datasets to provide visibility into our people following important processes around decommissioning assets as well*.

Omer Singer, Head of Cyber Security Strategy, Snowflake

This starting point will be the basis to determine where to keep the inventory going forward. If it’s a short list for a small company, an Excel or Google sheet will suffice.

Updates to the inventory can come from various internal sources, such as when procurement or IT requests and purchases new equipment, such as laptops or servers. Relevant personnel can send simple e-mails notifying the responsible party of the addition.

For more mature operations, submitting a ticketing system or, even better, automatically creating the configuration management database (CMDB) asset are good options. Make sure to include with relevant records the necessary data to identify it, such as its network address, hardware address, machine name, data asset owner, and department for each asset and whether the right personnel approved the asset’s connection to the network. Where possible, you should tie the software inventory into the hardware asset inventory so that you can track all devices and associated software from a single location.

Inventories must extend to include cloud components, software as a service (SaaS), platform as a service (PaaS), and infrastructure as service (IaaS). For SaaS specifically, this should include e-mail and web hosting solutions and HR platforms, marketing tools, legal platforms, and file repositories.

Adding and updating the inventory must also include removing unauthorized assets from the network. This process can entail physically removing systems or quarantining them via software methods to restrict their ability to communicate on the internet. Many current endpoint detection and response (EDR) solutions and some antivirus solutions provide this capability.

Inventorying every physical device and system you have means:

* actively managing all hardware devices on the network so that you give only authorized devices access, and
* finding unauthorized and unmanaged devices and preventing them from gaining access to your networks.

This inventory should include, at a minimum, all devices that have an IP address. But it should also include all assets with the potential to store or process information, including assets that you do not connect to a network. All these devices could be potential entry points for an attacker. Any weak link in the IT or OT chain can lead to further system vulnerabilities or even complete system compromise and takeover by hackers and attackers.

Among the traditional IT devices that you should include in this inventory are:

* desktops,
* laptops,
* mobile devices (you should segment employee devices – BYODs or “bring your own devices” – that connect or can connect to your networks),
* printers,
* databases,
* Windows and UNIX/Linux servers,
* backup systems,
* removable storage media, including USB devices,
* voice-over-IP telephone systems,
* storage area networks, and
* network equipment such as routers, switches, and firewall software.

As new Internet-of-Things (IoT) devices enter the home and workplace, your inventory should also consider these potential entry points into your system. Among the types of IP-connected devices that bad actors can quickly turn into attack vectors are:

* Voice-activated digital assistants such as Siri, Cortana, Google, or Alexa.
* Internet-connected industrial building systems such as HVAC systems, lighting systems, and so forth.
* Internet-connected appliances such as Wi-Fi-connected kitchen machines, including coffee makers, refrigerators, and ovens.

All organizations need to pay attention to traditional and emerging IT hardware assets and an extensive list of IoT devices and specialized equipment your organization uses. Although not all digital equipment is designed for connectivity to the internet, increasingly, many types of equipment, particularly newer models of gear, come with IP addresses or at least the potential for internet connectivity.

You’ll see in [Figure 1.1](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#c1-fig-0001) the types of equipment that you should consider including in your inventory in addition to the traditional IT assets. The items in this table are by no means exhaustive.



[**Figure 1.1**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#rc1-fig-0001) HARDWARE ASSETS.

Your organization may have greater or fewer types of equipment to include in your inventory. A dynamic host configuration protocol (DHCP) logging on all DHCP servers or IP address management tools can help update the organization’s hardware asset inventory.

Once you conduct the inventory, your job is not done. The inventory should be updated frequently to ensure accuracy. It is helpful to use an active discovery tool to identify devices connected to the organization’s network and update the hardware asset inventory.

Finally, all the inventory work can be made more accessible by a network monitoring system that alerts administrators to the presence on the network of unauthorized devices. These systems can scan the network and monitor systems on a 24/7 basis or at periodic intervals, looking for authorized and unauthorized devices and alert administrators to the network’s presence of unknown devices.

Many of these monitoring systems are free, but commercially available systems are options to consider. Without such network monitoring, employees can attach unauthorized devices to the network, defeating the purpose of developing the inventory in the first place.

You should conduct regular testing of the network monitoring system to see if the system catches all new hardware (or software, as we discuss in the next section) you add. You should remove or quarantine unauthorized assets until you update the inventory in a timely manner.

A helpful method for identifying unauthorized assets is to ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and note whether the assets are connected to the internet.

The following are some specific technical standards that might help IT specialists delve deeper into the subject of physical device inventory management:

**Relevant Technical Standards for ID.AM-1**

* CCS CSC 1
* COBIT 5 BAI09.01, BAI09.02
* ISA 62443-2-1:2009 4.2.3.4
* ISA 62443-3-3:2013 SR 7.8
* ISO/IEC 27001:2013 A.8.1.1, A.8.1.2
* NIST SP 800-53 Rev. 4 CM-8

**B.  Inventory Every Software Platform and Application You Use and Keep the Inventory Updated**

The NIST Framework subcategory that covers this aspect of cyber risk management is known as “ID.AM-2: Software platforms and applications within the organization are inventoried.”

Much like the concept of inventorying every physical device in the organization, creating a software inventory is crucial to:

* actively tracking all software on the network so that only authorized software is installed and can execute and
* helping to ensure unauthorized and unmanaged software is found and prevented from installation or execution.

Most organizations find that creating an inventory for software is more complicated than doing so for hardware. A wider variety of software is used, and trusted employees frequently download software. Still, software inventories should track all software used on general IT hardware such as:

* desktops,
* servers,
* workstations,
* laptops, and
* mobile devices owned by the organization.

In drawing up the software inventory, take a holistic view of your organization’s operations and functions to develop as comprehensive a list as possible for the software used in each chain of operations.

As is also true of hardware inventories, using an automated software inventory tracking tool can make the process far more comfortable and practical. This software tracking tool:

* can also be used to help pinpoint the installation of unauthorized or potentially unsafe software installed by employees,
* can help keep track of the software patches that most software suppliers issue on an ongoing basis, and
* can also help administrators implement white lists of software, barring employee installation of any software not on the white lists.

Just as is the case for hardware inventories, you should update software inventories regularly.

A good scenario would be to implement a combination of endpoint management and control by whitelisting or blacklisting software applications. End users will want the ability to access productivity tools, creating a central clearinghouse of software, either by an approved software depot (maybe a file share or website) or by a platform that publishes approved software that auto deploys for installation.

The software should be reviewed, tested (if possible), and approved before deployment to the repo (data repository) or, at the very least, installation. Ideally, each package deployed is currently supported by the vendor, or it’s tagged as unsupported. Unsupported software should find its way onto a deprecation list to sunset so the organization cannot carry technical “debt.” Also, tagging unsupported software helps with patching or vulnerability management, which we’ll get to in later subcategories.

If you’re tracking cloud applications, specifically SaaS, in an inventory aligned to ID.AM-1, there is no need to double count those applications in your software inventory.

You can build software inventories while meeting other security requirements. Implementation of endpoint detection and response (EDR) or some antivirus solutions should give you visibility into installed software across those covered assets. Running vulnerability management or scanning platforms should provide you with visibility into software installed in each scanned system. These systems can be combined or used by themselves to start gathering the deployed or installed software in your environment.

An ideal solution would be a single inventory with physical or virtual devices. You should record each software component installed on each device with the corresponding name, version number, install date, and current support status from the vendor.

The following technical standards list is worth exploring for learners who want to dig deeper into conducting and managing software inventories.

**Relevant Technical Standards for ID.AM-2**

* CCS CSC 2
* COBIT 5 BAI09.01, BAI09.02, BAI09.05
* ISA 62443-2-1:2009 4.2.3.4
* ISA 62443-3-3:2013 SR 7.8
* ISO/IEC 27001:2013 A.8.1.1, A.8.1.2

**C.  Prioritize Every Device, Software Platform, and Application Based on Importance**

This risk planning component entails developing criteria and assigning a priority rating to manage each logical control system’s risk. It is encompassed in the NIST subcategory of “ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.”

This prioritization means establishing formal access control used to assign a security level to an asset and determine which people can use it. You can devise any classification system to determine the priority levels that best suits your organization, and it doesn’t have to be tricky. Still, it does have to be specific enough to determine priority levels and achieve a ranking of importance. It can be as simple as “internal, external, and highly sensitive.” You should assign each asset to only one category, so make sure the categories are mutually exclusive.

This process of developing criteria for asset importance can be a conversation starter within the organization to draw out what is vital to the organization. Having a classification framework can engage people to explain what is essential to their work.

This process of engaging people to explain what is essential can help develop the prioritization scheme. A problematic component of this step is deciding which assets have the most business value. Many factors can come into play in determining where in the ranking any asset might fall.

Some factors to take into account when developing priority ratings might be:

* the role the asset plays in generating revenue,
* the degree of how integral the asset is to ongoing operations,
* how frequently bad actors target the asset for exploitation,
* how expensive the asset is to replace,
* how expensive the asset is to protect, and
* the reputational or legal damage that would ensue if the asset were compromised.

These factors are merely suggestions. You need to develop your priority list based on your unique circumstances and document how you created the priorities. The critical point is that you develop standard criteria for identifying the mission criticality of all assets.

When prioritizing assets, one thing to keep in mind is maintaining an inventory of all sensitive information stored, processed, or transmitted by the organization’s technology systems, including those located on site or at a remote service provider.

For more detailed technical help in this prioritization, the following standards and resources could be helpful:

**Relevant Technical Standards for ID.RA-5**

* COBIT 5 APO12.02
* ISO/IEC 27001:2013 A.12.6.1
* NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

**D.  Establish Personnel Security Requirements Including Third-Party Stakeholders**

This component of cyber risk planning and management maps to NIST’s subcategory “ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.”

Before you get to this activity, it’s advisable to create a security awareness program for all workforce members to complete regularly to ensure they understand and exhibit the necessary behaviors and skills to ensure the organization’s security. You should develop the organization’s security awareness program so that you communicate the central lessons engagingly.

In essence, establishing personnel security requirements means you decide which personnel at all levels, executives, management, staff, and third-party stakeholders (vendors, customers, and partners), have access to what assets, at what level of a security clearance, under what conditions. The importance of knowing who has access to various assets within your organization and outside your organization will only increase as the number of devices used and platforms over which content gets delivered grow. Without user-defined roles and responsibilities, the ability to maintain security across all surfaces is substantially weakened, particularly in times of system breaches and malfunctions.

Some essential tasks to undertake in defining workforce and third-party roles are:

* requiring third-party providers to comply with personnel security policies and procedures established by the organization,
* documenting personnel security requirements,
* defining minimum acceptable standards of information security requirements that you should include in all contracts (and adding addenda or exhibits for exceptional cases such as PCI – payment card industry – conditions), and
* establishing a right to audit clauses within contracts or through a third-party attestation.

Although establishing security requirements for organizational personnel is a relatively routine activity (e.g., few people within any organization have full admin privileges to critical systems), establishing those requirements for third-party providers can be challenging. Third-party providers are sometimes hard to identify and even more difficult to track regarding their personnel changes and security requirements.

Outside contractors, including IT support personnel, software developers, website designers, vendors, system support consultants, or any other third party that routinely require access to your organization’s network, should include in their agreements with your organization personnel requirements and security levels as are necessary for each person. All third parties should also be required to provide your organization with timely notification of any personnel changes as a routine matter.

The same procedures for informing employees, executives, and any other internal organizational staff of their security rights and responsibilities should also apply to third parties. This uniformity of using the same levels of information, rights, and responsibilities to both internal and external parties will help you more efficiently track and make necessary adjustments to the various levels of system security over time.

One of the crucial steps in establishing personnel security requirements is to gain buy-in from the organization’s top. An executive or someone within the leadership team must set the tone that cybersecurity is part of the organization through its training, development, implementation, and culture. Beyond setting the tone, someone must be designated to lead the cybersecurity program, assess the organization’s risks, map a plan to reduce those risks, and then execute that plan to reach a target state.

Whether your organization is small or large, you should designate personnel by role and name by their cybersecurity responsibilities. This designation will help immensely later on when you need to establish vulnerability management and incident response capabilities.

If you have valuable vendors or critical providers to your services identified, you should integrate them into your cybersecurity program. This integration holds even if you outsource your security to a managed security service provider (MSSP) or a security operations center (SOC).

The following technical standards are helpful resources for more technical insight into how best to establish and maintain personnel security requirements:

**Relevant Technical Standards for ID.AM-6**

* COBIT 5 APO01.02, DSS06.03
* ISA 62443-2-1:2009 4.3.2.3.3
* ISO/IEC 27001:2013 A.6.1.1
* NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

**III.  GOVERNANCE**

Cyber risk planning and management’s governance aspect covers the policies, procedures, and processes to manage and monitor your organization’s regulatory, legal, risk, environmental, and operational requirements. It’s a way of:

* defining a set of actions to protect against the threats and vulnerabilities your organization faces,
* establishing formal management policies, and
* seeing to it that they’re carried out on a day-to-day basis.

**A.  Make Sure You Educate Management about Risks**

One of the most critical aspects of governance for IT, cybersecurity, and other technical professionals to know is that you need to educate top management about cybersecurity risks so they can factor those risks into their decision-making. (This part of cyber risk planning and management aligns with the “ID.GV-4: Governance and risk management processes address cybersecurity risks” in the NIST Framework.)

As cybersecurity risks escalate, boards of directors and C-Suite executives are increasingly held responsible for managing cyber threats by shareholders and other stakeholders. In some industries, regulators are watching, which puts even more of an onus on top executives to stay informed.

**Voices of Experience
*On Governance***

**Know Your Laws and Regulations**

*The most important thing is to first understand which laws and regulations you need to comply with. That is really the baseline of what you need to know to understand and make sure that all the governance and policy structure covers your organization. It is different by industry, by size of your company, and the physical locations that you operate in. You also need to rely on your partners within the company, as you may not have all the answers. I know in my history, I have always had close relationships with both legal and HR. Coming from a life sciences background, Quality Control and E-discovery are integral partners on privacy issues to address the FDA regulations we had*.

Bill Roberts, former CISO at Hologic

So regardless of your organization’s size, developing a system for informing top decision-makers of cybersecurity risks will likely play an ever-more important part in your job. Your plan need not be elaborate or formal, and top-level decision-makers don’t need to become experts on technical matters. They do, however, need to understand the competitive implications of cybersecurity risk.

Once you’ve worked out a system for informing top management, the board of directors, or any relevant organizational committees, it’s important to schedule regular updates for these constituents. Suppose your organization is structured in a way that these top-level updates can’t easily take place. In that case, it might be worthwhile to create a cyber risk advisory council that can then provide reports or updates to the board and executive management.

One approach is to establish a dedicated information risk steering committee that validates your risk management program’s strategic direction and commits to appropriate resource levels and investments for addressing cybersecurity risks.

Ideally, an executive-level steering committee composed of business, regional, and functional leaders is accountable to the board of directors for the program’s success. It is responsible for providing the program leader with risk management direction. Overall, the goal should be to get cybersecurity viewed as an operational risk, not just an IT risk where leaders pass it off as merely a technical issue.

Many mom-and-pop and mid-sized organizations tend to outsource the management of cybersecurity risks. If that’s your situation, and you outsource to a cybersecurity vendor, good cybersecurity governance still requires you to develop a governance framework that keeps top management plugged into your particular risk profile.

We next include some references to help you learn more about applicable technical standards that could help you develop your organizations’ governance policy:

**Relevant Technical Standards for ID.GV-4**

* COBIT 5 DSS04.02
* ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3
* NIST SP 800-53 Rev. 4 PM-9, PM-11

**IV.  RISK ASSESSMENT AND MANAGEMENT**

A risk assessment is simply an effort to identify threats to your organization, how likely they are, and the consequences of the dangers. It would help if you used risk assessments to support your organization’s strategy, giving you the information you need to deploy specific practices and controls to address the risks you identify. They also help you assess how effective your procedures and rules for managing risks are.

Risk assessments typically precede risk management, which we will cover later. The best approach is to implement a risk assessment framework, which will help you develop objective measurements of risk and better protect at-risk assets. It would help if you used the risk assessment framework as a helpful guide for determining what is assessed, who needs to be involved, and the criteria for developing relative degrees of risk. In short, they are tools for making sense of what can be a very complex idea to implement.

Among some of the frameworks in use by other industries are:

* Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), from Carnegie Mellon University,
* NIST SP 800-30, Guide for Conducting Risk Assessments, and
* ISACA’s RISK IT (part of COBIT 5), ISO/IEC 27005:2011 (part of the ISO 27000 series that includes ISO 27001 and 27002).

**A.  Know Where You’re Vulnerable**

Identifying where your organization has vulnerabilities is a fundamental first step to conducting a full risk assessment. This aspect of cyber risk planning and management falls under the NIST Framework as “ID.RA-1: Asset vulnerabilities are identified and documented.”

The Council on Cybersecurity defines vulnerability assessments as an effort to “continuously acquire, assess, and take action on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.”[**1**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#c1-note-0001)

Knowing where you are vulnerable is contingent on having complete and updated hardware and software inventories. You cannot identify vulnerabilities on software and assets if you don’t know they exist. You can leverage automated tools and risk registers to document the risks associated with those assets.

Employees operating or overseeing the vulnerability management program for the organization should be trained on all the automated tools and methods to identify new vulnerabilities. They should also be responsible for the proper handling of vulnerabilities that are disclosed to the organization by third parties.

Investigating where you’re vulnerable can entail many activities, including:

* using vulnerability scanning tools through your organization’s systems and
* keeping abreast of vendor security alert announcements and periodic attack and penetration testing.

There is no one-size-fits-all approach for conducting vulnerability assessments because so much depends on your particular technical configuration, how large your organization is, and many other factors.

The following are some sound technical standards that might give you some ideas about implementing a sound vulnerability assessment initiative:

**Relevant Technical Standards for ID.RA-1**

* CCS CSC 4
* COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
* ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
* ISO/IEC 27001:2013 A.12.6.1, A.18.2.3
* NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

**B.  Identify the Threats You Face, Both Internally and Externally**

Once you’ve identified your vulnerabilities, a good next step is to identify the threats or kind of threats you most commonly face from both internal actors (e.g., disgruntled employees) and external attackers. This step in cyber risk planning and management dovetails with the NIST Framework’s subcategory “ID.RA-3: Threats, both internal and external, are identified and documented.”

A useful definitional distinction between assessing vulnerabilities and identifying threats could be helpful. Vulnerabilities are those aspects of your systems that attackers can exploit. Threats are the tools that attackers use to exploit those vulnerabilities.

It’s entirely possible to find vulnerabilities in your systems for which no threats or exploits seem to have been developed, and none seem likely on the horizon. The best means of identifying whether your vulnerabilities are targeted for exploitation and how best to deal with those vulnerabilities is to participate in established formal or informal information-sharing programs where your peers share the kind of threats they’ve experienced and how they have dealt with them. Participating in other cybersecurity forums and staying abreast of cybersecurity news are also means of identifying the threats you face.

Ideally, automated tools or systems should be in place to ensure that both internal and external threats are identified and eventually documented. If you can perform some fundamental threat modeling, this is a significant effort that will enhance your security posture.

Threat modeling could be as simple as taking a disgruntled employee and determining through a tabletop exercise the damage that employee could inflict on the organization. An essential step in this tabletop exercise would be to identify the vulnerable systems this employee would access. You could extend this exercise to external threats such as nation-states, if applicable, or commodity malware and other types of lower levels attacks.

The following are some technical standards that might help you delve deeper into the threat identification practices you could find helpful:

**Relevant Technical Standards for ID.RA-3**

* COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04
* ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12
* NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16

**C.  Focus on the Vulnerabilities and Threats That Are Most Likely AND Pose the Highest Risk to Assets**

This aspect of cyber risk planning and management appears in the NIST Framework subcategory of “ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.” In essence, this means that once you know where you’re vulnerable, the kind of threats you face, and the likelihood of those threats, focus on the vulnerabilities and threats with the highest risk to essential assets.

Some vulnerabilities will leave the organization open to more damage than other vulnerabilities, even if the likelihood of threats is low. Some threats will be minor annoyances, while others promise to shut down operations. Decide where the most significant risks to the most critical assets are and focus on those first.

For example, let’s say the chief criteria you use to rank the importance of assets are whether or not the asset is crucial to maintaining your e-commerce system’s reliability. Suppose your organization’s content server has vulnerabilities, but exploits of those vulnerabilities are unlikely. In that case, you may still rate that asset as highly important from a risk perspective because any threat to the content server, however low, could threaten e-commerce activity.

The reverse is also true. Let’s say your organization’s public address system has vulnerabilities, and the threat of exploitation is very high – your colleagues who use the same network have been hit with malware that cripples the same public address system. Despite this, you might rate this asset as lower in importance, despite the greater frequency of possible attack, because your chief goals are to maintain your e-commerce system, and your internal public address system outage won’t affect that system.

Using the criteria you developed for your assets’ importance, the next step is to determine your risk levels by factoring how likely those assets are to be successfully targeted.

[Figure 1.2](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#c1-fig-0002) might give you a sense of the risk prioritization involved in this step. As you can see, the level of threats and the value of the assets, however determined, can intersect in all kinds of ways to create high or low risks. It’s all a matter of how you score your assets and how you assess the likelihood of threats.



[**Figure 1.2**](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#rc1-fig-0002) Determining Threat Likelihood.

Some organizations may be willing to accept risks in some circumstances because the cost of addressing those risks may outweigh the foreseeable harm. These risks are referred to as residual risks but are tracked in the risk assessment process like higher-level risks.

For organizations short on time and personnel, several different methods determine your risk level for various assets. The simplest is using an excel spreadsheet to document the vulnerabilities and the likelihood and the potential impact that a known risk could have on a system or the organization.

Some useful tasks that should be helpful in risk prioritization are:

* using vulnerability scanning tools through your organization’s systems and
* keeping abreast of vendor security alert announcements and periodic attack and penetration testing.

The following technical standards could help develop this kind of risk determination:

**Relevant Technical Standards for ID.RA-5**

* COBIT 5 APO12.02
* ISO/IEC 27001:2013 A.12.6.1
* NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

**D.  Develop Plans for Dealing with the Highest Risks**

This final component of this chapter deals with efforts addressed in the NIST Framework subcategory “ID.RA-6: Risk responses are identified and prioritized” as well as “ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.”

Coming up with plans for dealing with the highest risks means figuring out what likely response you will have to the highest risk threats and coming up with some strategic options and actions for addressing those risks. Any response plans you have should be consistent with your organization’s goals (e.g., while implementing malware removal, you can’t just shut down access to e-commerce systems entirely, but you might be able to shut down other non-essential systems, such as invoice processing).

NIST lays out the process for dealing with the highest risks, saying that the organization should:

1. **1.** Implement a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
	1. **a.** are developed and maintained and
	2. **b.** document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the nation.
2. **2.** Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

This process requires that each option or action has an “owner” within the organization responsible for the activity, although a manager can delegate authority to subordinates, where appropriate. More importantly, this aspect of risk management should be viewed from an organizational perspective and highlights the need to bring in all stakeholders across the organization when developing response plans.

These assessments can take the form of scenario-testing, where hypothetical threats and risks are modeled on a role-playing or drill basis. Such scenario-testing or assessments can give an organization comfort that when real-world cybersecurity threats arise, the cyber risk planning and management efforts that you’ve undertaken have paid off in increased security and peace of mind.

It would help if you integrated information risk processes into day-to-day activities, like launching new products or services or adapting to a change in regulation or acquisition or other significant events. You can find further resources on this component of cyber risk planning and management in the following technical standards:

**Relevant Technical Standards for ID.RA-6**

* COBIT 5 APO12.05, APO13.02
* NIST SP 800-53 Rev. 4 PM-4, PM-9

**SUMMARY**

We’ve covered quite a bit of ground in this chapter. To recap, here are some of the highlights of cyber risk planning and management you’ve learned:

* Cyber risk planning and management are learning what can go wrong and the steps you can take to minimize the problems that might occur.
* The NIST Framework for Improving Critical Infrastructure Cybersecurity is a useful resource for developing your cyber risk planning and management strategies.
* Asset management can help you know what assets you have, keep track of them, and make sure you know which assets employees, vendors, and others have permission to use, all good foundations for cybersecurity risk planning and management.
* Hardware and software inventories are critical for prioritizing risk.
* Prioritizing risk requires developing a system for ranking the importance of organizational assets.
* Personnel at all levels, including third-party stakeholders, should be assigned to their access levels. Those levels determine who has access to what assets, at what level of security clearance, and under what conditions.
* Your organization’s top cybersecurity focus should be on those assets that are most important and face the highest risks.
* You should develop plans for the highest risks to the most critical assets, which you should coordinate and periodically test, with necessary internal and external personnel across the organization.

**CHAPTER QUIZ**

You might find the following short quiz fun to test your knowledge of risk management so far. You can find the correct answers at the end of the book.

1. **1. When it comes to planning for how you will deal with cybersecurity risks, what are the first steps your organization should take? (Select One)**
	1. **a.** Form a working group across the organization’s various departments (business, technical, legal, sales) to develop a plan.
	2. **b.** Make a list of the vulnerabilities we know we have and start building our plan to address those vulnerabilities.
	3. **c.** Conduct an inventory of all our hardware and software assets.
2. **2. Which of the following devices should you include in your asset inventory? (Select all that apply.)**
	1. **a.** Desktops, laptops, and servers.
	2. **b.** Mobile devices owned by the organization.
	3. **c.** Equipment specific to my organization connected to the internet or capable of being connected to the internet.
	4. **d.** All of the above.
3. **3. How should you deal with outside IT or tech vendors or other third parties regarding access to your networks? (Select one)**
	1. **a.** I make sure that all third parties who have access to my networks comply with personnel security policies and procedures with which my own organization’s employees must comply.
	2. **b.** Because the vendor is a leader in its field and many of my peers have recommended it, its cybersecurity policies are adequate to protect my organization.
	3. **c.** I limit access to my networks to only those IT or tech vendors I know well and have trusted in the past.
4. **4. When briefing management and decision-makers on the cybersecurity risks your organization faces, which of the following is the best approach? (Select one)**
	1. **a.** Explain the risk planning and management processes we’ve developed in detail to inform these decision-makers fully.
	2. **b.** Cut to the bottom-line to keep everything simple.
	3. **c.** Give them enough information to understand the competitive importance of cybersecurity risks and incorporate that understanding into business planning efforts.
5. **5. Which of the following is the best method for determining which assets rank highest in risk priority? (Select One)**
	1. **1.** Figure out where my organization is most vulnerable and rate those assets as the highest risk.
	2. **2.** Figure out which assets get breached or attacked most and rate those assets as the highest risk.
	3. **3.** Figure out the highest risk to important assets by factoring in those assets’ vulnerabilities and the degree of threats they face.
6. **6. Once you’ve figured out your highest priority risks, what is the best step toward managing those risks? (Select One)**
	1. **a.** Develop a response plan to adequately deal with the risks and make sure I inform top management of this plan.
	2. **b.** Form a group of internal and external key players across the organization to help formulate a response plan and then perform regular assessments of the plan after it has been developed.
	3. **c.** Hire an outside cybersecurity firm to come up with a plan and help manage the risks.

**ESSENTIAL READING ON CYBERSECURITY RISK MANAGEMENT**

1. **1.** NIST, SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012 at <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
2. **2.** Ken Sigler and James L. Rainey, III, *Securing an IT Organization through Governance, Risk Management, and Audit (Internal Audit and IT Audit)* Taylor & Francis, 2016).
3. **3.** Nicole M. Radziwill and Morgan C. Benton, Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management, *Software Quality Professional*, Vol. 19, No. 3, September (2017), arXiv:1707.02653 [cs.CR], <https://arxiv.org/abs/1707.02653>.
4. **4.** Alexander A. Ganin, Phuoc Quach, Mahesh Panwar, Zachary A. Collier, Jeffrey M. Keisler, Dayton Marchese, and Igor Linkov, Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management, *Risk Analysis*, September 5, 2017, <https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12891>.
5. **5.** Halima Ibrahim Kure and Shareeful Islam, Assets Focus Risk Management Framework for Critical Infrastructure Cybersecurity Risk Management, *IET Cyber-Physical Systems Theory and Applications*, June 3, 2019, <https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-cps.2018.5079>.

**Notes**

1. [1](https://learning.oreilly.com/library/view/cybersecurity-risk-management/9781119816287/c01.xhtml#rc1-note-0001) [https://www.cisecurity.org](https://www.cisecurity.org/).