How to Plan a Cybersecurity Roadmap in Four Steps

CIS Center for Internet Security®

CIS SecureSuite®

Contents

Executive Summary

Data breaches happen when we treat cybersecurity as a destination. If we believe security is complete, this can lead to wishful thinking versus security in the belief that your controls are complete. Security is never complete, however. In believing that it is, you could leave yourself vulnerable to a breach, as your posture may not necessarily relate to the threats bypassing static controls.

This is a problem, as the costs of a data breach continue to rise year after year. For example, IBM found that the average data breach cost $4.35 million in 2022. That's 2.6% higher than the previous year and 12.7% greater than the 2020 value. IBM also observed that 83% of organizations experienced more than one breach in 2022. In response to the costs of having suffered multiple breaches, 60% of respondents revealed that they had increased the price of their services and offerings.The costs identified above don't account for the reputational damages of a data breach, either. According to Varonis, 65% of consumers on average lost trust in an organization after it suffered a data breach. Such a dip in business can further strain the data breach victim, threatening its long-term viability.

Fortunately, we can minimize the risk of a data breach by approaching cybersecurity as a journey. It is a process. Even if you know you have work to do, you still need specific guidance to move toward a journey of success versus a journey of no progress. No cybersecurity journey is the same, after all. Yours is unique to you. If you have customers, their cybersecurity journey is unique to them.

To help you plan for your journey, we at the Center for Internet Security (CIS) have created this guide. Its purpose is to help you prepare for your cybersecurity journey so that you can avoid common obstacles and evolve your cybersecurity maturity as smoothly as possible. Over the course of the guide, you'll learn a four-step process for planning out your cybersecurity journey. You'll also receive tips on how you can map your evolving cybersecurity journey to our security best practices and other resources.

As you'll find out in the next chapter, it all begins with conceptualizing a cybersecurity roadmap.

Why Your Organization Needs a Cybersecurity Roadmap

VALUE AT A GLANCE

CIS SecureSuite comes with benefits, tools, and resources that can help guide you through the four-step process of creating a unique cybersecurity roadmap so that you don't have to go it alone.

Introduction

A spontaneous journey can be a lot of fun, but there's no question that it'll make for a bumpy ride at times. Movement with a plan of action will provide a much smoother journey. You'll be able to better visualize where you'd like to go and how you'd like to get there from where you are right now. As such, you need to be strategic and plan out your journey carefully. You can do so by creating a cybersecurity roadmap.

Let's take a moment to understand what a cybersecurity roadmap is and discuss some of the benefits of creating one.

ADVICE FROM AN EXPERT

The roadmap gives a perspective to stakeholders about the approach being taken to secure an organization and mitigate risk. The roadmap itself should be generalized to an extent to not be overly prescriptive. In essence, it shouldn't affect an organization's ability to alter the roadmap to address new risks or newly identified threats.

Sean Atkinson, CIS Chief Information Security Officer

Crafting a Vision for Your Cybersecurity Needs

A cybersecurity roadmap is an assessment of current capability and a gap analysis with a short- to long-term vision for integrating security practices. The need to address future implementation, control enablement, and a road to follow is critical for organizational and prioritization purposes. If you fail to plan, then plan for failure is the emphasis of this point. Looking at the roadmap for the journey will help you align to short-term destinations for control implementation and long-term strategies to assist in prioritization. Using this method of assessment and review will lead to efficiencies in building a risk-based plan for thwarting near-term gaps and long-term assessments of maturity in a security program.

The roadmap should delineate the predecessor tasks along the journey so controls and implementation complement a strategy of security and risk management. It should also give a perspective to stakeholders about the approach being taken to secure an organization and mitigate risk. The roadmap itself should be generalized to an extent to not be overly prescriptive. In essence, it shouldn't affect an organization's ability to alter the roadmap to address new risks or newly identified threats.

The ability to address agility is important. Prioritized items should be your first stops on the roadmap, but these can and often change in light of newly identified threats. For example, you might move up your long-term plans to replace a configuration management and control system after a new vulnerability arises, causing you to put your current plans on hold. Ultimately, you need to have the ability to recognize an issue and to address it as a current gap or part of the journey—even if you don't initially account for it.

TIP

The roadmap itself should be generalized to an extent to not be overly prescriptive. In essence, it shouldn't affect an organization's ability to alter the roadmap to address new risks or newly identified threats.

Four Main Steps to Create a Cybersecurity Roadmap that Grows with Your Business

Your cybersecurity roadmap will be unique to your organization. Even so, there's a set of steps that you can use to create a roadmap that fits your unique cybersecurity needs. They are as follows:

Know your needs to get packing:

Audit your environment to define a foundation for where you want to go.

Align to a framework to plan your route:

Identify a reference point that you can use to organize and plan your cybersecurity efforts around.

Implement your roadmap to hit the road:

Carry out the plan you have in place to achieve essential cyber hygiene.

Review, revise, and repeat to take a snapshot:

Examine the cybersecurity roadmap you implemented, revise and streamline, and start the process anew.

Fortunately, there are resources to help. CIS SecureSuite Membership provides what you need for your organization to move through these steps. It includes various benefits, tools, and resources for strengthening your cybersecurity posture and growing your cybersecurity maturity over time. Over the course of the next few chapters, we'll show you how you can use CIS SecureSuite Membership to create a roadmap that fits your unique needs.

RESOURCE

CIS SecureSuite Membership provides what you need for your organization to move through these steps. It includes various benefits, tools, and resources for strengthening your cybersecurity posture and growing your cybersecurity maturity over time.

Look to Your Cybersecurity Future

The roadmap is an outline of a detailed journey that only time will tell if the future-looking mapping is accurate or should be changed based on external stimuli to the cybersecurity program. Fortunately, this roadmap is yours and yours alone. You can adjust and build where needed so that it aligns with what you're facing and where you'd like to go.

TO-DO LIST

- ☐ Dive into our podcast discussion to learn more about cybersecurity roadmaps.

Know Your Needs

Get Packing for Your Cybersecurity Roadmap

VALUE AT A GLANCE

You need to know your needs to figure out where you want to go on your cybersecurity journey. CIS SecureSuite Membership gives you access to the CIS Critical Security Controls (CIS Controls) and related tools and resources that you can use to discover and manage your assets. That way, you can draw a roadmap, adjust it accordingly, and move onto the next steps.

Introduction

A roadmap for a journey is a fair metaphor for a cybersecurity improvement program if we allow for some nuance. In cybersecurity, the situation is a "dynamic" journey. Road conditions change constantly (like we notice in Waze). Many points on the journey that were once fixed can continually change. For instance:

- You might begin working with a new supplier and need to determine their cybersecurity risk posture.
- The regulatory environment might change, leaving you with the task of fulfilling a new compliance obligation or working with your customers to help them meet a new industry requirement.
- Your organization might deepen its understanding of the threats facing it, leading you to re-prioritize where you want to direct your security investments.

The first two considerations above are "normal" business challenges and opportunities that will affect your cybersecurity. A good cybersecurity improvement program (the journey) includes planning for change. For a supplier, a good definition and process for vetting and managing suppliers means that you can minimize the cost and risk of changing suppliers. For regulatory issues, a good program means that you will be able to adapt to new reporting requirements with minimal cost and complexity. The last — threats — means that better understanding allows you to adapt or change priorities as a normal part of business risk management.

All of these changes factor into your next stop along your journey. But every roadmap needs a starting point. In cybersecurity, the best place to start is for you to know your needs. Below, we'll discuss what this step involves, what challenges you might face as you get packing for the journey ahead, how you can overcome them, and how the CIS can help you.

Take a Broad View from Where You Are

You can't create a cybersecurity roadmap and act on it unless you figure out where you are first. In technical terms, we often refer to an "assessment" as a good place to start. But many assessments can get too granular too quickly. The business leadership is often not IT-savvy, so they might be tempted to spend too much time "counting the countable" — IT assets, servers, users, security incidents, etc. But the "fuzzier" stuff is really essential. They should be clear on their business purpose, key dependencies (like partners, suppliers, people), and how to manage them. This is just basic business.

With the business in mind, you can ask yourself the following questions:

- What is the purpose of your business?
- Which sources of information and/or services are critical to fulfilling the identified purpose of your business?
- What are your dependencies?
- What risks do they pose?

A lot of this requires teasing out implicit or unspoken assumptions. Many business owners assume that they understand their risks and dependencies. But every security incident tells us otherwise. Similarly, many assume that they are "too small to be a target"; ransomware tells us otherwise. On any given day in cyberspace, you're either a victim, a jump point on the way to the real victim, or an innocent bystander. None of us really knows which we are on any given day, but exploring your assumptions can begin to give you an idea.

Additionally, you might find the need to refine vague bumper stickers such as "Quality is job one" or "We are customer-driven" into specifics. Cyber defense is best seen as an ongoing improvement program. Every defender has a budget and a boss as well as constraints (like budget, personnel, and regulatory environment). So a successful program will have some short-term "wins" to establish credibility and momentum as well as some longer-term, foundational steps that can be built upon later. By taking both into account, you can gain valuable context that you can use to navigate the steps that follow.

ADVICE FROM AN EXPERT

We're not striving for perfection. What we're looking to do is get close enough to make reasonable business risk decisions at this moment in time. Those business risk decisions will ultimately change. But it's like having a cybersecurity roadmap in general. You need a place to start.

Tony Sager, CIS Sr. Vice President and Chief Evangelist

Tie the Business to Your Tech

Once you've gone through and evaluated your business, your mission, and your dependencies/risks, you must then take that solid understanding and match it to an inventory of what technology you have.

This is sometimes easier said than done. Most organizations find tech inventory to be challenging because they don't have the fundamental machinery in place to see and manage assets. It's more than a tech problem, as you must also have business processes in place to plan for, acquire, provision, and manage technology. Nor is it an exclusive security problem. It is about good asset management, which is similar to what you would expect for physical assets.

TIP

Once you've gone through and evaluated your business, your mission, and your dependencies/risks, you must then take that solid understanding and match it to an inventory of what technology you have.

These types of questions may come to mind:

- How many instances of a particular technology do I have?
- What condition are they in?
- Where are they located?
- How are they protected?
- Who is responsible for them?
- Who can access them?

Business owners ought to be asking the same types of questions they would ask about any physical or financial asset. We have tended to treat IT and cyber things as though there was magic or mystery involved. For example, it would be unacceptable to say we don't know much about our inventory of products, where they are, if they have been tested or not, and who is responsible for them, etc. In cyberspace, the assets are a mix of physical and "virtual," but the same questions apply. Keep in mind that developing an inventory isn't a task without its flaws. Inventory of hardware and software assets is a process and a machine, not an event. So you must design the machine to manage this information dynamically. And you want the information to be generated by, and provided by, technology. A clipboard of assets is a starting point if you have nothing else, but it's not sufficient.

Overall, people tend to get paralyzed when they realize that no inventory of hardware/software is perfect. But perfection is not an achievable goal. IT systems and their business use are dynamic, to say nothing of the tradecraft of attackers. The goal is to have visibility and control in a manageable way. Attackers have to live and operate in the same dynamic environment. If things never change, or they change under control, you actually make the attacker's job much more complex and risky for them. Remember that we don't even have perfect inventory of physical space. Many inventory programs or security measures that require having a solid inventory, such as app allow-listing and management of admin privileges, have failed — not due to a lack of technology but due to a lack of "management will."

What we're looking to do is get close enough to make reasonable business risk decisions at this moment in time. Those business risk decisions will ultimately change. But it's like having a cybersecurity roadmap in general. You need a place to start.

The Right Machinery for the Right "Management Will"

If you have the necessary motivation or "management will" to develop a solid inventory, you can find fundamental machinery that will help you. Take the CIS CIS Controls as an example. The CIS Controls provide a tested, vetted, transparent approach. They avoid security "magic" in favor of putting in place the foundations of good visibility and management. They do this right from the beginning with CIS Control 1: Inventory Control of Enterprise Assets and CIS Control 2: Inventory and Control of Software Assets. These security measures help you actively manage your enterprise and software assets to know what you need to monitor and protect.

As such, you can use both Controls to identify unauthorized and unmanaged assets and thereby minimize your risk of shadow IT.

You can implement CIS Controls 1 and 2 on your own. Alternatively, you can get even more support by becoming a CIS SecureSuite Member. CIS SecureSuite gives you access to additional tools and resources that you can use to prioritize your implementation of CIS Controls 1 and 2 down to the level of individual Safeguards. In this way, you can begin tracking your actions so that you can draw out the rest of your cybersecurity roadmap, adjust it accordingly, and advance efforts to meet complementary compliance requirements in the process.

RESOURCE

The CIS Controls provide a tested, vetted, transparent approach. They avoid security "magic" in favor of putting in place the foundations of good visibility and management.

The Next Step for Your Cybersecurity Roadmap

Using CIS Controls 1 and 2, you can build an inventory and start to think about whether the technology you're using is supporting your business mission and how they might be contributing to your risks. Such insight is crucial to packing for a cybersecurity roadmap that fits your unique needs and situation.

TO-DO LIST

- [ ] Assess your business.
- [ ] Use the following questions to tease out implicit/unspoken assumptions and refine vague bumper stickers about what the business does:
  - [ ] What is its purpose?
  - [ ] Which sources of information and/or services are critical to fulfilling that identified purpose?
  - [ ] What are your dependencies?
  - [ ] What risks do they pose?
- [ ] Assess your technology.
- [ ] Use CIS Controls 1 and 2 to map what you know about the business to what technology you have. (Note: DON'T strive for perfection.)
  - [ ] How many instances of a particular technology do I have?
  - [ ] What condition are they in?
  - [ ] Where are they located?
  - [ ] How are they protected?
  - [ ] Who is responsible for them?
  - [ ] Who can access them?
- [ ] Register for a webinar to learn how a CIS SecureSuite Membership can help you inventory your enterprise and software assets

Align to a Framework

Plan a Cybersecurity Roadmap's Route

VALUE AT A GLANCE

By aligning to a security framework, you can plan out your cybersecurity journey to follow a well-traveled route. This step is even easier when you use the CIS Community Defense Model, CIS Controls Navigator, and CIS Controls policy templates. These resources help you determine what CIS Controls make sense to your individual needs, map them to one or more security frameworks, and formalize their implementation with respective policies.

Introduction

Once you have an idea of where you are, you can plan the route for where you want to take your cybersecurity roadmap. A security framework is invaluable for this type of work. Let's clarify both what you stand to gain from aligning your cybersecurity roadmap to a security framework and how CIS can help you at this stage.

ADVICE FROM AN EXPERT

The advantage of aligning your or your customer's cybersecurity roadmap to a security framework is defining a road to follow using established security best practices. Think of it as referencing guideposts along your cybersecurity journey. They make it easier to reach a secure destination.

Sean Atkinson

The Value of Using a Framework

A cybersecurity framework is a set of best practices in the form of guidelines, standards, and instructions that's designed to address risk management and mitigation strategies implemented as controls. Just so we're clear, a framework is a well-traveled roadmap. Based on its construction, it can simply be a guide along your cybersecurity roadmap or define the route to be traveled.

Some common examples include the Payment Card Industry's Data Security Standard (PCI DSS) and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Our security best practices map to these and many more, as is evident in the image below.

Frameworks Provided with CIS Controls Mapping

- Australian Signals Directorate Essential Eight
- Azure Security Benchmark v3
- CISA Cybersecurity Performance Goals (CPGs)
- CMMC
- Criminal Justice Information Services (CJIS)
- CSA Cloud Controls Matrix v4
- Cyber Risk Institute (CRI) Profile v1.2
- FFIEC-CAT
- GSMA FS 31 Baseline Security Controls
- HIPAA
- ISACA COBIT 19
- ISO 27001:2022
- ISO/IEC 27002:2022
- MITRE ATT&CK v8.2
- NERC-CIP
- New Zealand Information Security Manual v3.5
- NYS Department of Financial Services 23 NYCRR Part 500
- NIST CSF
- NIST SP 800-53 R5
- NIST SP 800-171
- PCI DSS
- SOC 2
- TSA Security Defense Directive Pipeline
- UK Cyber Essentials
- UK National Cyber Security Centre (NCSC) Cyber Assessment v3.1

Industry Frameworks Referencing CIS Benchmarks

- DISA STIGs
- FedRAMP
- FFIEC
- FISMA
- PCI DSS

It follows that not using a framework to plan out your cybersecurity roadmap can be difficult. The challenge of doing this without a framework is twofold: one, where to start; and two, what to include. The vast array of security controls that exist is overwhelming, especially when compliance requirements and privacy regulations are also included. If the journey is building a risk-based control structure focused on security and a byproduct of compliance alignment, the stress of

identifying a starting point can lead to analysis paralysis. Should you start with low-hanging fruit such as a password policy, or should you address data classification as a first step? Using a roadmap to inherit and absorb a set of practices into an organization allows for better planning along with better integration of successive controls. The scope aspect of inclusion is also difficult, as managing a compliance program may miss respective elements of a complete security plan. The ability to contextualize the scope and the means of building momentum for a control plan itself will be a catalyst for improvement and maturity.

From a starting perspective, a good set of controls may include an implementation guide or provide a best practices document. You can learn from others and start to build an understanding of appetite and tolerance within an organization for control implementation. Using strategies that have worked for others allows a lead for security to build capabilities and also test the waters of security adoption in an organization. Simply applying a control will not be sufficient if the organization doesn't align with the practice.

A number of organizations provide implementation guides or best practices documents; other supporting organizations will also contribute in this space. From an inclusion standpoint, this can be very context-dependent for a respective organization, but generally, a set of security best practices from CIS or NIST provide a comprehensive plan that can be applied across multiple industries and businesses.

Without a security framework, you ultimately deprive yourself of learning from and applying this group experience to your individual case. Many other organizations are going through the same process you're going through. Using their example, you can streamline your own journey so that you avoid certain potholes and smooth out what you can.

TIP

From a starting perspective, a good set of controls may include an implementation guide or provide a best practices document. You can learn from others and start to build an understanding of appetite and tolerance within an organization for control implementation.

Exercising Care When Using a Framework

If you decide to align your cybersecurity roadmap to a security framework, it's important to keep in mind certain considerations.

The first is applicability to the organization's mission. Cybersecurity is a business risk and should be seen as such throughout an organization. With this in mind, the management of security controls is context-rich. It's a process of managing threats and mitigating risks when applying both a best practice and an achievable level of control.

The caveat to this previous statement is "achievable." It should be contextualized with respect to the risk an organization faces and the level of control implemented to mitigate the risk. If you know your opponent, you have a better chance of success. Take the saying, "Chance favors the prepared mind." Having an understanding of the risk allows you to address the risk with achievable levels of control. The emphasis is on "achievable," as this is a control that is one set in best practices but is not overly complex for the organization to adapt. If you have a fear of password compromise and you address it with multi-factor authentication (MFA), a complex password standard, and a change every 15 days, for example, the achievability is reduced. But if you address the issue with MFA, it may be enough to mitigate the risk and also not add layers of complexity to an organization.

Simultaneously, you need to think about how much control is needed to manage a risk appropriately. Too much control may inhibit business. This may get you into a situation where you're dealing with a phenomenon called the "Fog of More." In this situation, you end up overburdened by security tools and technologies that your ability to manage threats and mitigate risks begins to suffer. On the other hand, too little control may give a false sense of security. It's important to have the right balance.

TIP

Simultaneously, you need to think about how much control is needed to manage a risk appropriately.

The Need for Robust Security Frameworks

Given the challenges discussed above, it's important that you use a robust framework for planning the cybersecurity roadmap's route for yourself or helping your customers come up with a roadmap that works for them. Not all security frameworks are created equally, after all.

Specifically, you can look to the CIS Community Defense Model (CDM), the CIS Controls Navigator, and the CIS Controls policy templates. They all use a consensus-based and operational focused-approach that provides actionable controls for organizations to follow.

The CDM validates that the individual CIS Safeguards in IG1 defend against at least 75% of MITRE ATT&CK (sub-)techniques associated with malware, ransomware, web application hacking, insider and privilege misuse, and targeted intrusions. CDM thus confirms that you can use IG1 and the CIS Controls more generally to reduce your exposure to common threats.

Top 5 Attacks	IG1 CIS Safeguards Rate of defense against ATT&CK (Sub-)Techniques	All CIS Safeguards Rate of defense against ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Priviliege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Meanwhile, the Controls Navigator helps you visualize how the CIS Controls map to other security frameworks. In that way, you can use the CIS Controls to decide how best to align your cybersecurity roadmap to a framework if not multiple frameworks. This will help you to save time and money, as you won't need to duplicate efforts to comply with one framework and then another. You can address corresponding compliance obligations all at once—and all while strengthening your cyber defensive posture against common attacks.

Once you've decided the frameworks you'd like to align your roadmap to, you can then move on to the CIS Controls policy templates. These resources help walk you through the process of setting up policies for various critical security functions associated with the CIS Controls, including enterprise management, data protection, and security awareness training. With these templates, you can formalize what you've accomplished with the Controls thus far so that you can build upon your efforts going forward.

RESOURCE

The Controls Navigator helps you visualize how the CIS Controls map to other security frameworks. In that way, you can use the CIS Controls to decide how best to align your cybersecurity roadmap to a framework if not multiple frameworks.

The CIS Controls, the CIS Controls Navigator, the CDM, and the CIS Controls policy templates are available at no cost to users everywhere. But there's even more you can do with the CIS Controls via a CIS SecureSuite Membership. It comes with benefits, tools, and resources that you can use to prioritize and track your implementation of our security best practices. We'll dive deeper into these Membership benefits in the next section.

Simplify Your Use of a Framework

By using a security framework, you can plan out the route for your cybersecurity roadmap according to guideposts that others before you have set. In the process, you'll be able to make meaningful progress when it comes time to begin implementing your roadmap.

TO-DO LIST

- [ ] Identify a security framework (or frameworks) that are applicable to what you're trying to achieve, your industry, etc. As part of this process, consider the following:
  - [ ] Applicability to your organization's mission
  - [ ] Achievability based upon the level of risk confronting your organization and the level of control you'd need to implement to address that risk.
- [ ] Look to see if implementation guides and/or best practice documents are available for each of those frameworks.
- [ ] Use the CIS Controls Navigator and CDM to streamline the process of aligning to one or more frameworks while prioritizing cyber defense.
- [ ] Check out this page to learn how a CIS SecureSuite Membership can help you use the CIS Controls and related resources.

Hit the Road

Implement Your Cybersecurity Roadmap

VALUE AT A GLANCE

To implement your cybersecurity roadmap, you need a place to start. CIS SecureSuite Membership provides you access to CIS CSAT Pro, a tool which can help you lay a foundation of essential cyber hygiene using the CIS Controls. It also comes with access to CIS-CAT Pro, which saves you time and effort by automatically evaluating your systems' settings against the security recommendations of the CIS Benchmarks. Together, these tools streamline your assessment, auditing, and reporting capabilities. They also help you move onto the last step of creating a cybersecurity roadmap.

Introduction

Now is the time when you're ready to hit the road and put your cybersecurity roadmap into action. But you might have questions. Where do you start? How do you get the most out of this implementation phase?

Here, we'll identify a goal toward which your first step enacting your cybersecurity roadmap can lead. We'll then pinpoint how you can build upon this progress to travel even further with your cybersecurity maturity.

Start with Essential Cyber Hygiene

By taking care with where you're heading when you hit the road, you can lay a foundation of continual growth for your cybersecurity roadmap. You can do this by starting with cyber hygiene.

It's easy to dismiss cyber hygiene as unimportant or less interesting. The marketplace is noisy and "foggy," with lots of grand claims and hype. But every analysis of real-world attacks reaches the same conclusion: most attacks and the conditions that enable them are variations of well-known patterns of attacks. And basic, well-defined steps will prevent, block, or limit the vast majority of attacks. These defensive steps can sometimes be operationally challenging and take time. But they are problems that typically don't age well, and so you need to get started.

An analogy of public health applies. We wash our hands at certain points in the day NOT because we know for certain that it stops a specific named bacteria but because it is a foundational, behavioral step that can block the transmission vectors for a large class of problems. We engage

in other behaviors, like avoiding sick or coughing people or getting our shots, for similar reasons. So cyber hygiene is loosely equivalent — it's the set of things that represent the foundations of defense, that should be part of the report for any useful security assessment, and that translate complex and confusing science into specific, high-value behaviors.

That said, without a specific definition, "cyber hygiene" is just a bumper sticker usually tossed out with some examples. For example, "We all need better cyber hygiene managing administrative privilege."

At CIS, we''ve focused on defining cyber hygiene story through Implementation Groups. A definition becomes the basis for a plan along with a way to start measuring progress, communicate with management, and compare progress against others.

That's why we recommend *essential* cyber hygiene, as embodied in Implementation Group 1 (IG1) of the CIS Controls. Our analysis is clear — there is tremendous security value in a set of foundational steps no matter how risky or complex your business situation. This is evident in CIS CDM. Indeed, by implementing IG1 Safeguards, you can defend against 77% of MITRE ATT&CK (sub-)techniques associated with today's top attack varieties. These include malware, ransomware, web application hacking, insider and privilege misuse, as well as targeted intrusions.

Top 5 Attacks	IG1 CIS Safeguards Rate of defense against ATT&CK (Sub-)Techniques	All CIS Safeguards Rate of defense against ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Priviliege Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Focus on Secure Configuration Management

As you make your way through IG1 of the CIS Controls, you'll quickly find the need to manage your systems' secure configurations. CIS Control 4 is all about managing the secure configurations of your enterprise and software assets, after all. Even so, secure configuration management isn't unique to the CIS Controls. A fundamental security practice called out in every security framework (including the CIS Controls) is to manage the security configuration of IT components.

What is unique is the way CIS can help you harden your systems' configuration. At CIS, we call these configuration guides CIS Benchmarks — and we are the world's largest independent producer of this type of guidance. The CIS Benchmarks provide a vetted, trusted, industry-adopted basis for managing IT components. They don't just provide consensus-driven recommendations for securing your systems. They also tell you the importance, the security benefit, and how you can prove that you've implemented each of those secure configurations.

To illustrate, the figure to the right shows what a "maximum password age" requirement looks like in CIS Microsoft Windows 10 Enterprise Benchmark v2.0.0.

All CIS Benchmarks are mapped to the CIS Controls — including IG1 — at the recommendation level upon their release. This helps you harden your systems in accordance with essential cyber hygiene across your environments.

1.1.2 (L1) Ensure 'Maximum password age' is set to '365 or fewer days, but not 0' (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This policy setting defines how long a user can use their password before it expires.

Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

The recommended state for this setting is `365 or fewer days, but not 0.`

Note: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the **Default Domain Policy** GPO in order to be globally in effect on **domain** user accounts as their default behavior. If these settings are configured in another GPO, they will only affect **local** user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Rationale:

The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user has authorized access.

Impact:

If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

ADVICE FROM AN EXPERT

A well-designed "machine" of IT and security automation is a key component of security reporting and compliance. It should produce most of the evidence and data needed to demonstrate the effectiveness of your security program or the security program of your customers to others (e.g., management, auditors, regulators).

Tony Sager

Automate Your Hardening Efforts

As we discussed in the previous section, CIS Benchmarks (either directly or through cloud images) are a tremendous starting point — industry-accepted with demonstrable security value. But they must also be actively managed. You need to start from a CIS Benchmark as an enterprise standard and modify it as necessary for specific challenges. For instance, maybe you need to run legacy apps that require specific ports open, get management approval, and then implement and continuously measure and manage them by identifying and correcting unapproved changes as well as reporting on status. More broadly, they also become part of your purchasing and software development decisions (Will this app run on my hardened systems?) and your IT policies.

All of this establishes the need for a designed program of automation, reporting, and correction. That's why automation, based on standards, has been a theme of the CIS Controls since their inception. It should produce most of the evidence and data needed to demonstrate the effectiveness of your security program or the security program of your customers to others (e.g., management, auditor, regulators).

We've grown up to think of assessment, auditing, and reporting as "episodic" or a "snapshot" — something that happens as a special occasion outside of real work. In fact, given the dynamics of the IT and business worlds, we should instead design our enterprises to be

TIP

Given the dynamics of the IT and business worlds, we should design our enterprises to be continuously measured, reporting, and adapting. The goal is to spend most of our attention and resources on business work and less of it on "proving we did the right thing."

continuously measured, reporting, and adapting. The goal is to spend most of our attention and resources on business work and less of it on "proving we did the right thing." In this spirit, we've designed CIS SecureSuite to provide Members with access to automation capabilities. Take the pro version of our Configuration Assessment Tool (CIS-CAT Pro), as an example. CIS-CAT Pro helps you run automated scans of your system's settings against the security recommendations of the CIS Benchmarks, saving you time and money when taking a secure configuration policy and implementing it across your environment.

Additionally, we've designed CIS SecureSuite to help Members with reporting and making corrections as necessary. Such is the case with the pro version of our Controls Self Assessment Tool (CIS CSAT Pro). It's designed to help you track and prioritize your implementation of the CIS Controls v7.1 or v8. By identifying your current capabilities and gaps, you can use that information to evaluate which Safeguards you've implemented, assign tasks for new implementation tasks, and adjust accordingly as you make your way through the Implementation Groups of the CIS Controls.

RESOURCE

CIS-CAT Pro helps you run automated scans of your system's settings against the security recommendations of the CIS Benchmarks, saving you time and money when taking a secure configuration policy and implementing it across your environment.

Gaining Ground Through Your Cybersecurity Roadmap

Enacting your cybersecurity roadmap is a journey. You can't finish it all at once. By hitting the road and starting off with essential cyber hygiene through the CIS Controls, you can move on to manage your systems' secure configurations via the CIS Benchmarks. From there, you can streamline your implementation of both using CIS-CAT Pro, CIS CSAT Pro, and other resources of a CIS SecureSuite Membership.

TO-DO LIST

- [ ] Establish essential cyber hygiene at your organization.
  - [ ] Work your way through the Safeguards in Implementation Group 1 (IG1) of the CIS Controls that will have the greatest impact for your organization.
- [ ] Implement CIS Benchmarks to securely configure the systems you've deployed.
- [ ] Apply for a CIS SecureSuite Membership.
- [ ] Refine your implementation of our security best practices.
  - [ ] Use CIS-CAT Pro to automatically evaluate your systems' settings against the security recommendations of the CIS Benchmarks.
  - [ ] Leverage CIS CSAT Pro to prioritize, track, and evolve your program to implement the CIS Controls.

Review, Revise, Repeat

Snapshot Your Cybersecurity Roadmap

VALUE AT A GLANCE

A true cybersecurity journey is never over. As you evaluate your results and start the process anew, you can use CIS SecureSuite Membership to save even more time and effort. For instance, CIS Build Kits help you to automatically implement the remediation recommendations of the CIS Benchmarks, while CIS WorkBench serves as a centralized location from which you can download member resources, tailor the Benchmarks to your individual needs, as well as collaborate with other Members and cybersecurity experts.

Introduction

You've reached the last step of your cybersecurity roadmap: review, revise, and repeat. It's here that you take a snapshot of your cybersecurity roadmap. At this point in your road trip, you've reached an attraction toward which you've been journeying. Doing so has changed your perspective, putting you in a position where you can examine what you've implemented, revise and streamline, and start the process anew onto the next attraction. Let's discuss how you can use this last step as a means to continually strengthen your cybersecurity posture.

Evaluation: The Key to Contextualizing Implementation

Any controls plan and any risk assessment require curation not just at the beginning of implementation but through the operational lifecycle. Auditing, threat assessment, gap analysis, and changes to your organization's infrastructure need to be ingested as part of a robust program. That's why you need to take the time to evaluate your efforts and measure the impact.

If you don't, you can't account for the dynamic array of threats and risks confronting you and/or your customers. Indeed, the consequence of "set it and forget it" has dire consequences, as the false sense of security is undermined in an ecosystem of continuous discovery and utility of vulnerabilities and threat vectors. As we said in the first installment of this series, cybersecurity is a journey, not a destination.

Evaluation serves another key function as part of your cybersecurity roadmap: it also leads to the formation of a new roadmap. Improvements and assessment will require reengineering of a

controls program. Threats and risk change, and a contributing change is needed within the control infrastructure to reflect these changes.

The same can be said of business strategy and how the security program complements the business. The refinement of the roadmap reflects continuous improvement and progression through obstacles along the roadmap journey. Some can be planned along the journey, and some are surprises. Being agile enough to address each requires preparation and understanding the objectives of redefining the cybersecurity roadmap. As you account for new obstacles and requirements, you can revise your cybersecurity roadmap to take you in new directions, building upon your success as you go.

ADVICE FROM AN EXPERT

Reducing the drag of a control will only help it integrate more fully and be accepted by your organization and respective stakeholders. If system access becomes too cumbersome or process too inhibiting, users of the processes will find alternate ways of bypassing the controls.

Sean Atkinson

Streamline Your Cybersecurity Processes Where You Can

Given the fact that your cybersecurity journey is constantly evolving, you need to find areas where you can streamline your efforts. Doing so will save you time, money, and effort. You free your security professionals from tedious tasks so that they can take up more important duties.

Naturally, this affects your cybersecurity posture, too. Reducing the drag of a control will only help it integrate more fully and be accepted by your organization and respective stakeholders. If system access becomes too cumbersome or processes too inhibiting, users of the processes will find alternate ways of bypassing the controls. In essence, internally you have created a red team

TIP

Any controls plan and any risk assessment require curation not just at the beginning of implementation but through the operational lifecycle.

strategy to take a well-defined control but ultimately go backward on the roadmap. If your control infrastructure is bypassed, then you have no control. Losing visibility into processes of control is an area of control maintenance. Is the control effective, working as intended, and battle-hardened in a way that addresses the risk? With these elements, you know you have a good control in place. If you are missing the utility of the control and it is not effective and bypassed, then the effort and risk mitigation is lost. It will lead to greater security concerns in terms of the bypassed method becoming a new risk. Thus, you have a new destination on your journey to solve.

For example, the most secure corporate Wi-Fi has people switching to guest Wi-Fi to bypass restrictions and control, therefore wasting time in implementation, but also identifying that the control isn't integrated with the business. If the corporate Wi-Fi is bypassed with control to necessitate access control, data management, and posture assessment, those controls are thwarted and missing if those same corporate devices are allowed to use a less secured network. The energy and time in creating a control are also sunk costs, as the requirements for protection and in this case the cost of security are missing. Awareness becomes critical for both the implementer of the control and the user of a corporate system.

It might be difficult to streamline things on your own. Fortunately, CIS is here to help.

Our CIS SecureSuite Membership includes tools, benefits, and resources for helping you to implement security best practices such as the CIS Controls and the CIS Benchmarks. Take the CIS Build Kits as an example. Available as Group Policy Objects (GPOs) for Windows and Bash shell scripts for Linux, CIS Build Kits automate the "Remediation" section of the CIS Benchmarks PDF document. Such functionality helps you automate the hardening of your systems to a majority of a CIS Benchmark's recommendations, thereby saving manual effort.

CIS WorkBench is another Membership resource for streamlining your cybersecurity efforts. It serves as a central hub for collaborating and downloading Membership tools and resources, including XML, Excel, OVAL, and Word versions of the CIS Benchmarks. Through CIS WorkBench, you can also tailor your CIS Benchmark settings so that you can continue your cybersecurity journey according to your unique goals.

RESOURCE

Available as Group Policy Objects (GPOs) for Windows and Bash shell scripts for Linux, CIS Build Kits automate the "Remediation" section of the CIS Benchmarks PDF document.

Navigating an Ever-changing Destination

It's been mentioned before, and is worth mentioning again; cybersecurity is a journey, not a destination. It's important to keep in mind that the velocity of change and the ever-increased surface area of attack contributes to the narrative of continuous improvement. Adversaries will continue to attack as it is in their interests (hacktivism, nation-state, etc.) or ultimately for some adversaries (cybercriminals) a very profitable business. A similar adage is that the attacker only has to be right once and the defender right all the time to address cyber risk and vulnerability.

Let CIS SecureSuite guide you every step of the way from now to long into the distance, enabling you to drive your cybersecurity roadmap home.

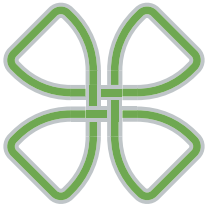
TO-DO LIST

- ☐ Apply for a CIS SecureSuite Membership.
- ☐ Evaluate how far you've come to see where you can streamline your efforts.
  - ☐ Use CIS Build Kits to automate the "Remediation" section of the CIS Benchmarks.
  - ☐ Access CIS WorkBench to download additional Membership benefits, tools, and resources.
- ☐ Use where you are now to understand your current needs and goals.
  - ☐ Repeat the process of creating, aligning, working through, and revising your cybersecurity roadmap.

Conclusion

There exists an unfair balance of defending systems compared to adversarial activity, leading us down the road of due diligence and the practice of strong cybersecurity. CIS SecureSuite includes benefits, tools, and resources that can help you balance the odds in favor of your organization.

May this Irish blessing we've revised guide your cybersecurity roadmap and journey going forward:



May the path be cleared for progress.
May the framework lead the way.
May the controls work in tandem to defend our secure domain as
The risk falls short of exploit and the attacker fails again.

About the Authors

Sean Atkinson
CIS Chief Information Security Officer

Sean is Chief Information Security Officer of CIS. He uses his broad cybersecurity expertise to direct strategy, operations, and policy to protect CIS's enterprise of information assets. His job responsibilities include risk management, communications, applications, and infrastructure. Prior to CIS, Sean served as the Global Information Security Compliance Officer for GLOBALFOUNDRIES, serving Governance, Risk and Compliance (GRC) across the globe. He also led the security implementation for the New York State Statewide Financial System (SFS) from 2007 to 2014 before his role as Internal Control, Risk and Information Security Manager.

In addition to his work with CIS, Sean is also an adjunct professor of Computer Science at the College of Saint Rose in Albany, New York.

Tony Sager
CIS Senior Vice President and Chief Evangelist

Tony is a volunteer in numerous cyber community service activities and serves as an inaugural member of the DHS/CISA Cyber Safety Review Board, an advisor to the Minnesota Cyber Summit, and a member of advisory boards for several local schools and colleges. He is also a former member of the National Academy of Sciences Cyber Resilience Forum and serves on numerous national-level study groups and advisory panels.

Tony retired from the National Security Agency in 2012 after 34 years as a mathematician, computer scientist, and executive manager. As one of the Agency's first Software Vulnerability Analysts, he helped create and lead two premier NSA cyber defense organizations (the System and Network Attack Center and the Vulnerability Analysis and Operations Group). In 2001, Sager led the release of NSA security guidance to the public and expanded NSA's role in the development of open standards for security. Sager's awards and commendations at NSA include the Presidential Rank Award at the Meritorious Level (twice) and the NSA Exceptional Civilian Service Award. The groups he led at NSA were recognized for mission excellence inside government and across industry with awards from numerous sources, including the SANS Institute, SC Magazine, and Government Executive Magazine.

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

To learn more, visit www.cisecurity.org.

CIS Center for Internet Security®

CIS SecureSuite®

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security

@CISecurity
TheCISecurity
cisecurity