Confidence in the Connected World

CIS® Center for Internet Security®

A CISO's Guide to Bolstering Cybersecurity Posture

By Sean Atkinson, CISO, CIS

CISO eBook

Contents

Introduction

The CISO blog launched on the CIS website in January 2018. Since then it has provided guidance on a number of cybersecurity topics with a special focus on the importance and implementation of the CIS Controls™, a collaboratively developed, prioritized set of actions to protect your organization and data from known cyber attack vectors.

This book is a compilation of some of the blog posts in one place for easy reference. It begins with an introduction to cybersecurity approaches and then moves into identifying and calculating risk. In today’s world, risk and data protection go hand-in-hand; that’s the third section of the book. Finally, we conclude with some cybersecurity implementation strategies.

The book is organized so that you can easily jump to the section that most interests you. Some of the original posts have been edited for content and length. If you find this book valuable, you may wish to read the original and future CISO blog posts at https://www.cisecurity.org/.

CHAPTER 1: APPROACHES TO CYBERSECURITY

Breaking the Divide Between Governance and Operational Cybersecurity

Governance in cybersecurity

Governance describes the policies and processes that determine how organizations detect, prevent, and respond to cyber incidents. Many organizations have a division between governance and management. Those who work in governance tend to emphasize strategic planning, whereas operational management deals with the day-to-day operationalized approach to security. Sometimes this results in different leadership perspectives.

Making the organizational move from a divided hierarchy to one in which strategy informs operation (and operation informs strategy) is a difficult challenge. Communication is key to effectively managing expectations, messaging, and security posture throughout the process.

Governance
strategic planning

Operational Management
day-to-day approach

Detect, prioritize, and control

Operational controls – the real-life response to a cybersecurity incident – should be the focus of any security program. Managing these controls and reporting to a governance structure may not require the knowledge of operationalization. Instead, it may rely on an agreed-upon level of risk management involving both governance and operational leadership.

Operational controls managers should measure their security posture against a framework or baseline such as the CIS Controls or NIST Cyber Security Framework. Understanding your organization's compliance levels is key to finding weaknesses in the organizational controls as well as the prioritization of investment for strengthening controls.

With clearer reporting and analysis of risk reduction, we can bridge the gap between governance and operational security, leading to better strategic decision making and a more unified approach to the cyber threat landscape.

The Fox and the Hedgehog: Strategic Cybersecurity Response Planning

Risk managers can use security controls to implement processes to limit the vulnerabilities, risks, and threats that abound in the physical and cyber space. Let’s define the strategic plan of the implementation of such a systematic approach.

The fox and the hedgehog

A singular vision of the end goal must be in place for any plan of action to be effective. A plan of control and measurement should define risk mitigation and provide evidence that security controls are in place.

In the security world, there are two popular approaches: the fox and the hedgehog. Where a “hedgehog” approach tends to take a singular view of security, the “fox” will review security situations from multiple perspectives. The strategic planning work of Isaiah Berlin, for example, follows the hedgehog style.

In order to develop policy ideas into a singular vision, try implementing a document framework. I prefer to utilize a three-tiered framework based on:

- Policy
- Standard
- Procedure

Start with a singular “control” and a single document that details the information security policy which defines that security control. Next, document the details of how to implement that control. Ensure you take into account multiple cybersecurity approaches and concepts such as access control and data protection for a multi-layered, defense-in-depth methodology. By taking a single idea and approaching it from multiple views, the “fox” style comes back into play.

Breaking down the tenets of cybersecurity

Many organizations implement multiple security standards and controls. The CIS Controls, for example, provide 20 security best practices. Each best practice has its own connotations for implementing and measuring compliance to a specific task.

Implement controls by breaking the standards down further into a procedure. In most cases, each security procedure you plan should have a singular implementation strategy and control. Role-based access control (RBAC) is one popular and effective way to implement controls, ensuring that only authorized individuals can access control systems. RBAC is based on the user's role within the organization to implement specific security controls.

Hedgehog, fox, or both?

It's interesting to note that one must play both roles – hedgehog and fox – at particular points throughout cybersecurity assessments and audits. The hedgehog approach comes into play when working with a singular vision and "the one important thing" (a particular security control). However, the multitude of ways to implement a particular control requires a multi-disciplined fox approach. Put simply, to achieve the singular you must know and understand multiple concepts. Both approaches are required to build a strong cyber defense.

CHAPTER 2: RISK

The Risk Conversation

Our day-to-day business activities often don't involve a specific focus on information security and making good decisions based on risk and controls. The spectrum of risk management duties often falls through the hierarchy based on a top-down process. As this happens, the roles and responsibilities that make up risk management may slip through the cracks. It is here that we must identify the stakeholders of risk management. We must also consider those within business processes who can make a big difference between a foiled attack and a catastrophic security incident.

Risk and the organizational culture

Risk elicitation (or risk gathering) at only the senior level of an organization is a common mistake. A better solution is to implement a collaborative intake process to identify risks throughout all levels of the organization. Without this view, it's likely that some risks may not be uncovered until a security assessment or penetration test identifies them – or worse, a breach occurs.

Regularly poll internal stakeholders for their opinions about risk or use scenario-based discussions to identify risk. The CIS Controls can also be used to discover gaps in security that could be articulated as risks. Start a conversation with those responsible to implement those controls technically, operationally, and/or physically.

Getting to the scenario response

Intake of risk analysis can take many forms, from simply asking:

- How is our network at risk?
- What is the biggest risk you see to the network?
- How would this particular risk occur?
- Can we stop a malware outbreak and what is our response time?
- If we were to download a malicious file, what is our mean time to detection, response, and eradication?

The aim here is to ask questions that require a scenario response. This leads to a deeper dive into an answer rather than just "yes" or "no." Fault tree review, discussed later, is a technique using a starting scenario and an engaged audience to lead to uncovering and discovering risks across business processes, technical functions, and operational controls.

The process of risk management can be intimidating at first. By asking a few questions, you can begin to develop a baseline and understand the threats facing your organization.

View the CIS Cybersecurity Threats page

Where Risks Meet Controls

Using the CIS Controls to define and identify risk

The CIS Controls are a set of prioritized set of actions to protect your organization and data from known cyber attack vectors. They are developed and maintained by a global community of cybersecurity experts.

Aligning an organization's internal security controls to a consensus-based collection of cyber-risk mitigation strategies like the CIS Controls can help improve cybersecurity posture. The integration of a risk management program with the CIS Controls can define how a company identifies risk and how it can be treated. Treatment strategies come in the form of remediation steps to lower exposure to risk from vulnerabilities and threats to computer systems and business processes.

How the CIS Controls can help

CIS Controls Version 7, released in 2018, contains a total of 20 Controls. How each CIS Control is implemented will vary by organization. To define the need for a Control, a risk that needs to be treated must be present. Identification of these risks may go undetected by many organizations, and so the CIS Controls can provide a helpful starting point of evaluation.

Basic CIS Control

CIS Control 1: Inventory and Control of Hardware Assets

Your organization can gain major insights into its risk identification and management by turning each of the CIS Controls into a question and analyzing your answers to each. Start by reviewing CIS Control 1 – Inventory and Control of Hardware Assets – as part of a risk identification exercise:

Question: Can your organization define and detail all its hardware assets? Be sure to include laptops, bring-your-own-device (BYOD) mobile devices, and printers.

Asking this question can generate additional scenarios to identify risk:

- Are there any connected assets which are not authorized to be on your network?
- Are all assets configured securely?
- What role does each asset play in your organization's processes?
- What data is stored on each asset?

These are high-level ideas to start the conversation in regards to risk and its identification. The use of the CIS Controls can generate questions that identify gaps and weaknesses. Use them to implement a level of risk management and respective control over your organization's assets, data and systems.

Download the CIS Controls

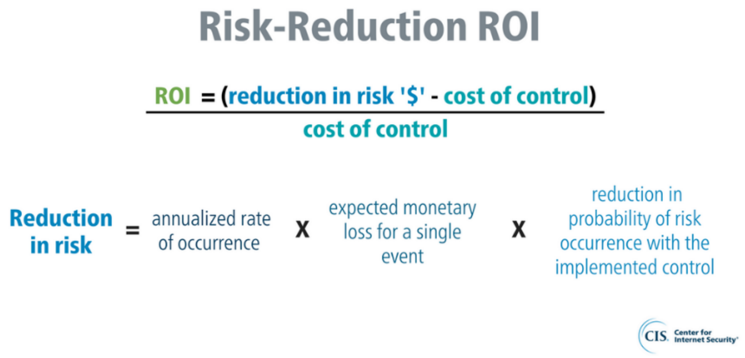
The One Equation You Need to Calculate Risk-Reduction ROI

Evaluating internal systems and services is a key component to understanding your organization's security posture. One methodology is measuring your risk against the CIS Controls to determine the strength and weaknesses of risk treatment. Put simply, once you understand your risks, you'll have a better idea of what it will take to proactively address them.

Inevitably there will be gaps – not just in your security processes and implementations, but also in the measurement of control effectiveness. These gaps should be identified and managed as action items to improve the overall security posture of your organization. The determining factor for many organizations is where to focus effort. Start by asking, "What will have the *greatest* effect on reducing risk?"

Calculating risk-reduction ROI

With any security decision, implementing new solutions and controls will likely require a monetary expense. This is where you'll benefit from the ability to determine the cost of a potential risk versus the cost of the control. Here's one way to calculate return on investment (ROI) to account for the cost of risk vs the cost of control:



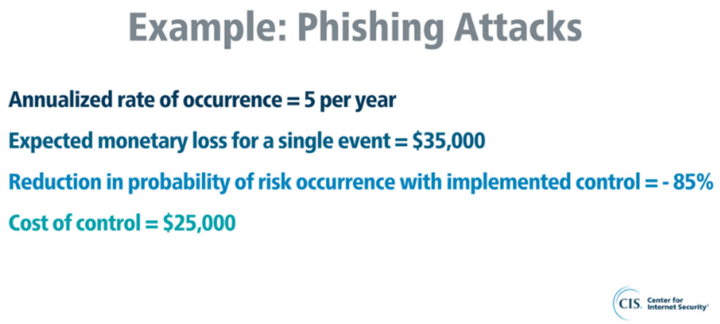
Risk-Reduction ROI

$$\text{ROI} = \frac{(\text{reduction in risk '\$'} - \text{cost of control})}{\text{cost of control}}$$

$$\text{Reduction in risk} = \text{annualized rate of occurrence} \times \text{expected monetary loss for a single event} \times \text{reduction in probability of risk occurrence with the implemented control}$$

ROI example

Let’s use phishing attacks as an example. Say your organization expects to get phished 5 times per year, at an estimated cost of $35,000 per successful attack. The cost to train employees to spot and avoid phishing emails is expected to be $25,000. Here’s what the security ROI would look like:



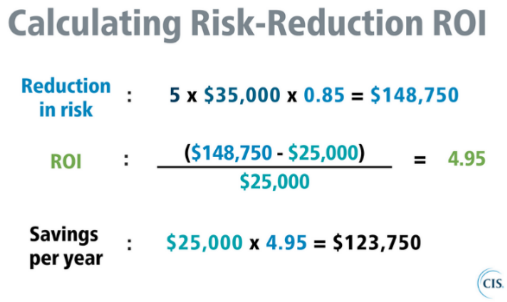
Example: Phishing Attacks

Annualized rate of occurrence = 5 per year

Expected monetary loss for a single event = $35,000

Reduction in probability of risk occurrence with implemented control = - 85%

Cost of control = $25,000



Calculating Risk-Reduction ROI

$$\text{Reduction in risk} : 5 \times \$35{,}000 \times 0.85 = \$148{,}750$$

$$\text{ROI} : \frac{(\$148{,}750 - \$25{,}000)}{\$25{,}000} = 4.95$$

$$\text{Savings per year} : \$25{,}000 \times 4.95 = \$123{,}750$$

In this example, it makes monetary sense to invest the $25,000 in training to help reduce the risk of a successful phishing attack. Remember that each organization is different, and determining these variables will be based on circumstance and risk tolerance of the organization. As with any application of the CIS Controls, the cost to implement will depend on the estimation of risk reduction and other local factors.

Setting priorities

Looking into multiple cybersecurity solutions for the same risk? To compare mitigation strategies, run each one through the risk-reduction ROI formula above and determine which is best at reducing your risk surface. You can also use this formula to determine which risks are the most cost-effective to address and which will help prioritize your defense strategy.

Of course, any strategy must also be calibrated against the business' operational and organizational goals, with respect to the risk of greatest importance or control deemed most crucial for cybersecurity. Nevertheless, this equation will prove useful in helping your organization review the cost of solutions per technical control.

Fault Trees and Risk Forests

Risk management and the elicitation of scenarios

Gather the appropriate stakeholders to start a risk-focused discussion. Be sure to focus on forecasted expectations and what should occur in your organization if those expectations fail to meet the forecast.

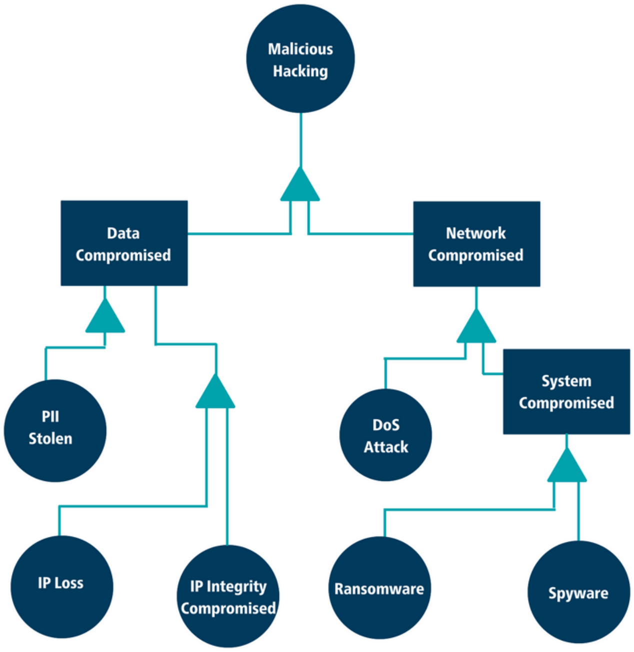
Use the following concepts to build a risk elicitation questionnaire, interview, or peer review:

- **Risk triggers** – Questions to review the underlying assumptions of currently-held beliefs.
- **Scenarios based on the triggers** – Diagrammatic examples that will require weighted responses to a risk scenario.

Building a fault tree

Use the responses from the questionnaire to begin to build a fault tree to see where risks to the organization are greatest and how you might respond. Start building the fault tree using a specific high-level event, then determine the responses to risk using weighted examples.

The example in the diagram shows potential responses to malicious hacking. This scenario is used to determine whether the data within the organization is the most likely to be compromised or if the systems would be the most likely target.



Given this analysis we can then look at the corresponding events that would lead the organization to the main outcome of malicious hacking. To build the tree, entertain multiple scenarios of how the top-level event could occur. In this tree we have restricted the number of potential leading events for brevity.

Responding to risk

After you've built out your fault tree it's time to consider how your organization will respond to potential risk. If the data stolen is personally identifiable information (PII) such as phone numbers and home addresses, what is the duty of care to inform those whose data was stolen? If the data was intellectual property (IP), what is its value to the organization and how much was taken? These questions will put you on the journey to incident response and implementing protective controls for data loss prevention as mitigation strategies for risk.

As you move from outcomes to causes in the diagram, your organization can:

- Evaluate existing controls and risk management processes
- Determine the organization's current risk posture
- Strategize about the future implementation of controls based on the likelihood and probability of compromise in the event of a data breach or technical failure

To greater improve your cybersecurity posture, consider developing multiple control scenarios for each event. You may want to follow existing best practices like the CIS Controls or frameworks such as NIST CSF.

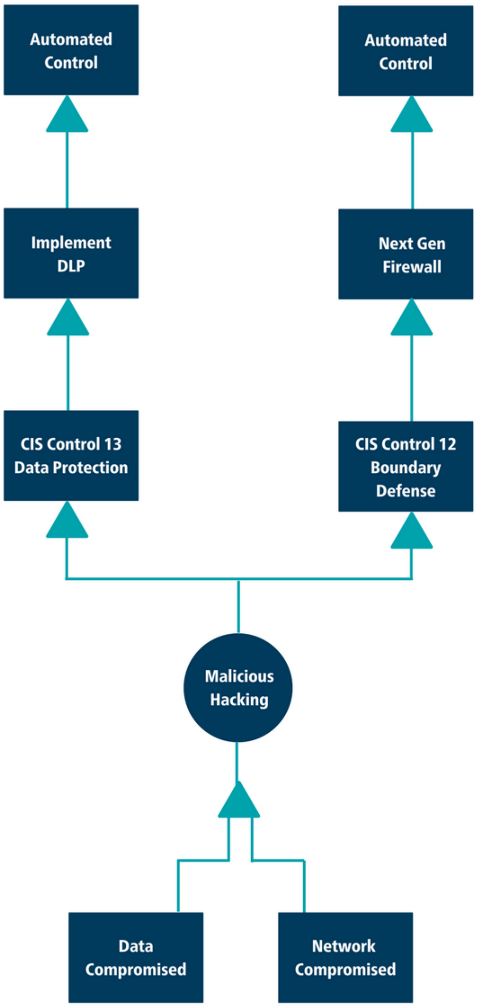
Creating Event Trees to Help Measure Control Effectiveness

The transformation of a fault tree

Part of determining the best strategy for a set of controls involves employing techniques to evaluate the risk-reduction ROI as well as a review of measuring the effectiveness of the control. The next step is to transform the fault tree into an event tree. The event tree will help you create mitigation strategies for those faults you wish to control. It's a helpful strategy for improving your organization's security posture.

Building an event tree

To start our example, we will use the left side of the event tree in the following diagram:



In this example, data from the organization has been compromised due to malicious hacking. There are specific CIS Controls which can help prevent such a scenario from taking place and remediate the risk of a data compromise.

Measuring probability

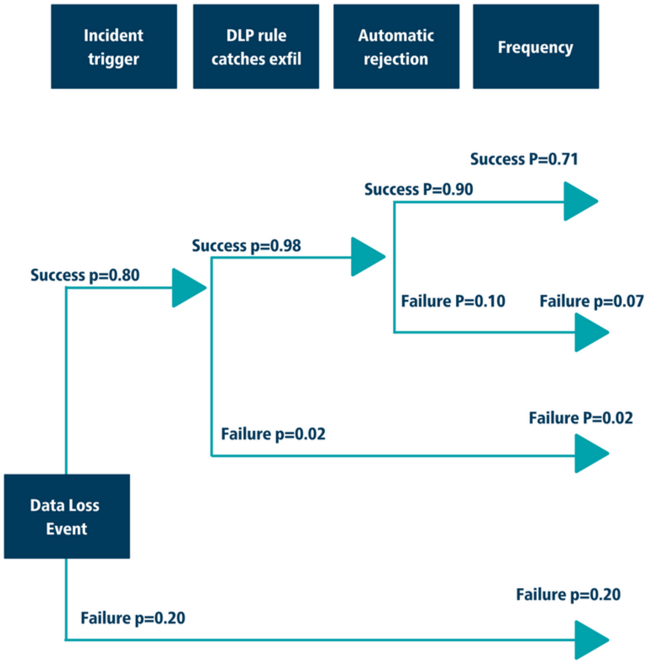
Because no security control is 100% effective, each organization will need to establish a baseline for the probability of failure. This measurement will have to be gauged over time in order to provide the correct probabilities.

Here is an example set of data protection probability figures:

Event	Identified exfiltration	Total tests	% Probability (P)
Event triggered	128	160	0.80
Caught exfiltration	157	160	0.98
Auto rejection	144	160	0.90

Event	Domain	Result
Data exfiltration	NA	P = 1.00
Incident not triggered	Fail	P = 0.2
Incident triggered	Success	P = 1 – 0.2 = 0.8
DLP doesn’t catch exfil	Fail	P = 0.02 (1-0.98)
DLP catch exfil	Success	P = 0.98
Auto rejection fails	Fail	P = 0.10 (1-0.90)
Auto rejection works	Success	P = 0.90

Next, apply the probability to the diagram below to evaluate overall risk.



By mapping out the total probabilities, we can see that the organization’s total success probability during the 3-step event is 71% compared to a total failure probability of 29%. From a risk perspective, the company needs to decide, “Are we implementing a strong enough set of security controls to across a particular platform to successfully implement the CIS Control 13 level of data protection?”

Each company’s requirements are different, but these types of evaluations will allow for a more stringent review of risk.

Risk and response

The aim of these exercises is to contemplate your organization’s risk and response activities. Allow for the review of multiple probabilities to understand risk mitigation strategies and their effective ROI.

CHAPTER 3: DATA PRIVACY AND PROTECTION

Response Planning and Data Privacy

Spectre, Meltdown, and response planning

2018 saw multiple attack vectors at play and organizations recognizing a need to respond. Patches for Spectre and Meltdown were deployed in environments around the world. Emergency management communication has also been a central focus of response planning.

From stories of the mismanagement of an entire organization's "distribution list" to public photos of passwords written on sticky notes, cases of bad cyber hygiene abound. Nevertheless, these cases make great examples for new employee security training and annual cybersecurity training refreshers.

2018: The year of data privacy

2018 was a year of 'data privacy." The EU General Data Protection Regulation (GDPR) came into fruition at the end of May, providing us with an opportunity to improve our data handling processes. As we progress and complete the impact analysis and measure of risk, we need to understand how data flows through our respective organizations.

There are areas around data handling which every organization will need to review and fine-tune. Some questions to start your investigation:

- **What data do we have?**
- **How do we use it?**
- **Where is it stored and processed?**

The answers to these questions will form a reference point for your organization to gain a controlled foothold over its data and information management processes. Your specific industry dictates the type of data you have (payment information, customer data, health records, etc.). The type will produce different answers. Still, the questions need to be asked, understood, and documented in a data protection plan (DPP). If you don't have a DPP in place, now's the time to start developing one.

Getting ready for the future

No matter what the future holds, you can improve your cyber defenses by implementing critical patches immediately and ensuring systems are up-to-date. Developing a DPP is another great step to take. A DPP can help with:

- Day-to-day management of information
- Preparing your organization for any future breach or incident which may occur

- Ensuring data within an organization is properly defined, labeled, and controlled
- Mitigating against ransomware attacks by limiting an attacker's access to sensitive data

Webinar: Where Privacy Meets Security

GDPR and Data Privacy

With privacy in mind, let's examine the General Data Protection Regulation (GDPR). The requirements under the GDPR have provided a new compliance path for many organizations around the globe. This path has multiple steps in order to conform to the regulatory requirement. Let's take a look at how organizations can take the first few steps towards GDPR compliance.

Who's managing and accessing your data?

Think about the data your organization manages and how it is processed. Whether data management is an internal function or outsourced, if you are making decisions about how you collect data and how it is processed within your organization, you are a data controller.

The data controller is a specific role in GDPR. However, if you process requests for such actions (data processing or management) from a customer or data provider then it is more likely you are in the data processor role. No matter which roles apply to your organization, if your company handles EU citizens' personal data, GDPR compliance is still required.

What data is now considered "personal"?

Personally identifiable information (PII) consists of typical data elements plus some other items that you may not have considered:

Personal data

- Basic identity information such as name, address, and ID numbers
- Web data 'online identifiers' such as location, IP address, cookie data, and RFID

Special Personal Data

- Health and genetic data
- Biometric data
- Racial or ethnic data
- Political opinions
- Sexual orientation

What is the intent of these privacy controls?

The purpose of GDPR is to institute specific controls in regards to how personal data is treated. The main focus is to create a set of standard operating procedure as it pertains to how personal data is managed within organizations.

Examples of such requirements are:

- **Mandatory breach notifications** – Requires a fast response or organizations could face large fines.
- **The "Right to be forgotten"** – Necessitating the "ability to be found".
- **Consumer profiling restrictions** – Personal data should not be used without consent, a specific approach to opt-in, and the ability to opt-out of consent for organizations to utilize personal data.
- **Be accountable for your data** – Conduct a privacy impact assessment to determine what type of personal data is handled, processed, and stored, and for what purpose.
- **Access to personal data** – Right to access; data should be controlled based on a "need to know" basis.
- **Right to rectification** – Right to update personal data and correct inaccuracies.
- **Privacy by design** – New functions and elements of future processing capability or personal data management must utilize this as a non-functional requirement in the conceptualization of the business process.

What should organizations do?

Several steps are required and each organization should review the GDPR to ensure specific requirements are met. Here are some key steps that can help you achieve GDPR compliance:

- **Conduct a privacy impact assessment** – This assessment will show you what data the organization owns which is personal data or special personal data.
- **Examine data flows** – Know where your data is, who has access to it, and for how long you keep it.
- **Conduct a risk assessment** – Based on the privacy impact assessment and the data flow review, you'll emerge with a clearer picture of what risks the organization is accepting.

- **Implement privacy by design** – With GDPR, privacy must now be a consideration in change management, implementation of new systems, or business processes that handle PII.
- **Implement security controls and measures** – Employee training and security controls can help protect data.
- **Working with third parties** – If you engage data processors or controllers as part of your business, make sure to require GDPR compliance. If a failure in the third party processes reveals PII to those who do not have a need to know, your organization will also be held liable.
- **Hire a Data Protection Officer (DPO)** – Hire or assign the responsibility of a DPO; this role can encompass the responsibility of GDPR requirements.

How can CIS help?

CIS has numerous resources which can help your organization work towards GDPR compliance.

CIS SecureSuite® Membership: Includes access to CIS-CAT Pro Assessor configuration assessment tool, CIS-CAT Pro Dashboard web application with enhanced reporting features, remediation kits for rapid implementation of secure CIS Benchmark configurations, and more.

CIS Hardened Images™: Bringing the security of the CIS Benchmarks™ to cloud computing environments on AWS Marketplace, Microsoft Azure, and Google Cloud Platform.

CIS Controls: Prioritized best practices and policy guidance to help organizations defend against the vast majority of cyber threats.

Download our white paper: Are You GDPR Ready?

Using CIS Control 13 to Create a Data Protection Plan

CIS Control 13: Data Protection helps identify elements that would comprise a solid data protection plan (DPP).

Elements of a DPP

- **Objective** – Specific to organizational security policies or regulatory controls such as GDPR/NIST.

- **Roles and responsibilities** – Addresses key roles in the organization and the data protection responsibilities of each.
- **Data protection risks** – Identifies potential security risks as related to sensitive data.
- **Acceptable use policies** – Apply to different classes of data within an organization.
- **Data storage requirements** – Must consider how to manage the storage size of data (including backups!).
- **Data utilization** – Addresses how data is used within the organization.
- **Data integrity and assurance** – Examines how to securely store and transfer data.

How CIS Control 13 can help

CIS Control 13 recommends the following steps to define and control data:

- **Identification of sensitive data** – You first have to know what data is sensitive in your organization before you can determine what requisite controls need to be in place.
- **Apply controls to systems that house or transport the data identified above** – Now that sensitive data has been identified, safeguards must be deployed to protect the data in transit and at rest.
- **Data loss prevention (DLP)** – Data is the lifeblood of any organization and it changes constantly for internal processes, updates, new information, etc. The importance of DLP is to control the flow of data and make sure its utilization is approved, controlled and monitored.
- **Threat detection** – Once your organization has implemented the sub-controls defined above, a scenario-based risk assessment should be performed to manage data exfiltration and misuse. For example, ask yourself, "Should deployed endpoints and servers have read/write capability to USB devices?" If for your organization the answer is 'NO', then disabling or providing detection software will reduce the risk of exfiltration through such a method.

These are high-level ideas that can help ensure that data privacy is defined and controlled within any organization. As multiple requirements for compliance are often in play and cybersecurity best practices are paramount, a strong DPP can help your organization identify risks and define a plan of action.

Learn more about CIS Control 13: Data Protection

CHAPTER 4: STRENGTHENING CYBERSECURITY POSTURE

How Security Controls Can Improve Your Cybersecurity Posture

Security is a journey, not a destination. It is important to understand that as security and IT introduce critical configurations and security controls, management will be required over time. A single audit of a configuration in the deployment of a new system is an important check in the beginning phase. It’s equally important to confirm over time that your initial deployment configurations are still accurate and compliant.

Measuring compliance

CIS offers two helpful resources that organizations can use to improve their cybersecurity posture. CIS Benchmarks are secure configuration guidelines and CIS-CAT is a configuration assessment tool. These tools align control with functionality and security with compliance.

The first step for any organization is to establish a baseline of security. This will be the secure image for any system deployed within an IT environment. There can be hundreds of different configuration checks necessary to secure a particular operating system, server, or mobile device – this is where the free CIS Benchmarks recommendations can be extremely helpful. These recommendations are developed through hours of discussion and debate through our global community of volunteers via CIS WorkBench.

Are you a cloud-enabled enterprise? Check out CIS Hardened Images for a secure baseline. They’re available on AWS Marketplace, Microsoft Azure, and Google Cloud Platform.

Once you’ve established a secure baseline for your image, it’s time to see how it stacks up to the CIS Benchmarks. CIS-CAT Lite, our free tool, and CIS-CAT Pro, available through CIS SecureSuite Membership, both allow users to measure their compliance to the CIS Benchmark recommendations.

Register for the next CIS-CAT Pro webinar

Continuous monitoring

Once you've confirmed compliance to a baseline, there are two continuous monitoring items to consider:

1. **"Regular cadence" monitoring** – This involves rechecking the systems to confirm their deployed compliant status is still in effect. How often this monitoring takes place could be based on criticality of the system, the size of data centers, or other factors. For example, critical systems may require weekly or monthly reviews while a large data operation may only require annual monitoring.
2. **Change management** – This comes into play when a configuration is needed (such as the installation of particular applications or software) that is not aligned to the secure baseline. In these cases, the required change should be documented as part of a change management process. Be sure to document the impact of any configuration change on your system by running another compliance scan after the change has been implemented.

Paying attention to the process

If we maintain a process of control, compliance, and monitoring, it will allow for the creation of a complete asset management process, a configuration profile for deployed systems, and a managed process for incorporating changes into the system. Each part of this process will increase overall cyber hygiene and provide the impetus for maturing an information security program. Tools like CIS-CAT Pro can help organizations along the path to security and compliance.

→ Learn more about CIS SecureSuite Membership

Compliance in Multifaceted Environments

It has become a common practice to combine management of different technologies into a single process and expect that actions taken will occur in the same manner and time frame as when those processes were separate.

Compliance - with conditions!

At CIS we align best practices to processes and actions as a requirement. For IT teams, it is crucial to understand your hardware and software environments in order to maintain asset inventory and know what systems you have. Patching, updates, and remediating issues with configurations are all items that are specifically prescribed by CIS as basic elements of establishing and, more importantly, maintaining security control.

Issues may arise when the expectation is that management of Windows and *nix environments (such as Unix and Linux) are the same: “Just update and make sure we are compliant.” If only it were so simple! In most cases, these processes (updating, vulnerability scanning, configuration management, etc.) should be specifically managed with respect to the underlying technologies.

The devil is truly in the details. Specific controls and compliance requirements are set against each type of infrastructure. Therefore, automation and management of checks across the infrastructure is recommended. This will allow for a strategized solution to different pathways of patch management as well as define those systems where there are levels of criticality for securing infrastructure.

Critical patch management

In some cases, such as industrial control systems, the technologies involved are so critical that patch management cycles are built around a specific downtime. This leads to a conglomeration of patches all to be installed at a single point in time. Our warning when dealing with such critical systems is twofold:

1. Test those patches in another environment for operational effectiveness
2. Have a “back out” strategy should things go awry

It is not often that you will find a test environment that is an exact mirror of production, which means that testing can only go so far. For this reason, we suggest that technical teams always have a strategy to implement stability and re-apply a particular patch or update once the correct implementation strategy has been identified.

→ CIS Cybersecurity Minute: Positive Effects of Patching

Cloud Compliance – How to Stay Secure on an Intangible Infrastructure

“If it is not my device, how do I control it?”

Security in the cloud can be a contentious topic. It has been challenging for users to define a set of criteria for cloud computing security and then be able to attest to its compliance. Over the past five years, cloud computing has become a strategic plan of action for many organizations, combining on-premises infrastructure with a virtual cloud network.

The appeal of cloud computing is hard to deny as a value proposition. It provides scalable infrastructure, on-demand responsiveness, and (based on the cloud provider) a multitude of services that augment the IT landscape. A key point to consider is that security is just as important in the cloud as it is on-prem.

Any strong IT security program will require that the following main areas are covered:

- Governance and policy
- Asset management
- Access control
- System development and maintenance
- Incident response
- Business continuity

No matter the cloud provider, you'll need to confirm that controls are in place addressing the topics above. Each of these topics can be addressed to ensure controls and a measurable level of compliance. With a relatively simple approach to each, you can work with cloud providers and maintain a level of compliant and auditable control over your virtual network.

Compliance in the cloud

Let's examine each of the security topics in more detail and find a way to ensure security is top-of-mind in cloud computing environments.

Governance and policy: As a standard, leading cloud providers maintain compliance and security controls as part of their infrastructure. In some cases, this means the users employ a risk strategy – that is, the user undertakes a certain amount of risk by transferring the security requirements to the cloud provider(s). Check the cloud services agreement for details and don't be afraid to ask about security processes and policies.

It's worth noting that the roles and responsibilities for maintaining security will depend upon the platform, infrastructure, and software-as-a-service model selected by the user. This will influence the level of ownership and security responsibility for both the cloud provider and customer.

Asset management: In order to successfully manage your assets, you'll want a record of what systems are deployed as well as any security level which may be defined for those systems. Some tips:

- Manage the addition of new instances through a change control process
- Assign ownership of assets
- Monitor any cloud account(s) through the provider's management console and with your own organization's accounts payable

Access control: As with any system, role-based security is paramount. Nothing changes with a cloud implementation in this case; you'll want to audit, review, and control access based on a user's "need to know" and RBAC.

System development and maintenance: Start this process by applying secure configuration standards like the CIS Benchmarks to any cloud-based environments. CIS Hardened Images are pre-configured virtual machines for a variety of platforms and technologies. Using such pre-configured secure images saves time over manually hardening a virtual machine. CIS Hardened Images allow for the deployment of already compliant systems for a variety business purposes. For those developing software in the cloud, CIS Hardened Images provide convenient security from the start. Once secure configurations are in place, maintenance to prevent "configuration drift" is the next step; regularly compare cloud configurations to the "golden" hardened image as part of your control framework.

Incident response: Communication is key when there is an incident in the cloud. Be sure to understand what role the user and cloud provider play in a security incident, as well as what the cloud provider can supply in terms of data. This response strategy may be utilized for testing the incident response process and ensuring both organizations know how the cloud provider's supplied data will be utilized. The response strategy should be approved and documented within your organization's incident response plan.

Business continuity: Consider what will happen if one or more of the systems upon which your organization relies fails. One of the many benefits of using cloud infrastructure is the ability to shift data quickly depending on your needs – should a natural disaster strike a main office, cloud-based services will run unaffected. However, you'll want to consider your cloud provider's resiliency and disaster recovery strategy. What are their guarantees and limitations in regards to "up time?" Based on this response, porting data to another cloud provider may be part of your organization's business continuity strategy.

Don't go it alone

Working in the cloud allows often provides organizations flexibility and convenience to scale their resources as needed. It also means working with others – such as cloud providers and IT staff – to ensure security measures are being implemented on the virtual network. Be sure to look into helpful resources like the CIS Hardened Images to help your organization stay secure in the cloud, and don't be afraid to ask questions about your cloud provider's security processes and procedures. With security in mind, the cloud can be a helpful extension of your organization's IT infrastructure.

Explore CIS Hardened Images

Discovering Security Gaps with Vulnerability Management Controls

Asking the question, "Where are my gaps and have I been tested?"

The process of managing an infrastructure and its security posture will require an approach that focuses on what hardware and software exist within my environment and ensures that it is authorized. CIS Control 1 and CIS Control 2 focus on creating and maintaining an inventory of approved hardware and software. You'll want to revisit those recommendations if you're just starting a security program.

Patching

It is at this point that we want to make sure that the approved and authorized infrastructure (including desktop computers, printers, routers/switches, and mobile devices) is secure. Over time software and firmware versions become outdated and require patching as new vulnerabilities are identified. "Patching" simply means applying updates to software or firmware, typically to remediate security flaws.

Patching is a cyclical process and must be done consistently. If it's not, the organization's exposure factor increases along with the risk of potential exploitation.

Applying CIS Control 3

To manage the risks presented by application vulnerabilities, implement CIS Control 3: Continuous Vulnerability Management. Here are some helpful tips:

- **Implement automated vulnerability scanning.** Make sure to cover your entire infrastructure and use authenticated scanning where possible.
  - When selecting a vulnerability scanner, require a SCAP validated software that assesses security configurations. For more on vulnerability scanners, check out Common Configuration Enumeration CCE. Find an updated list of code vulnerabilities here: Common Vulnerabilities and Exposures CVE.
- **Don't simply scan; take action** when the assessment results are presented from the scan and remediate any vulnerabilities discovered. Remember, these are not just reports, they are actionable intelligence for improving your security posture.
- **Ensure your vulnerability scanner stays up-to-date**: in order to provide the most accurate results, it too will need updating to make sure it has the latest vulnerabilities.

- **Compare your results over time**: Develop a security baseline of assessment results to show that identified vulnerabilities are being remediated over time. This will ensure your business risk is understood, reported, and accepted by the appropriate risk owner.

Is this all I have to do to be secure?

Unfortunately, there is no silver bullet for cybersecurity. CIS Control 3 helps organizations define, enumerate, and remediate known vulnerabilities. Each of the CIS Controls will require time to implement and focused attention in order to have a greater chance of thwarting exposure, exploit, and compromise of your systems.

→ Try CIS-CAT Lite, a demo of CIS-CAT Pro, a SCAP-validated configuration assessment tool

Implementing Secure Configurations with Remediation Kits

Resources like the CIS Benchmarks and CIS-CAT Pro help organizations around the world start secure and stay secure. The CIS-CAT Pro Assessor tool scans against a target system’s configuration settings and reports the system’s compliance to the corresponding CIS Benchmark. While it’s great to know where your systems stand, manually implementing the recommendations can be a daunting task. Another method for implementing the configuration guidelines recommended in the CIS Benchmarks is via remediation kits, which help users automate the process.

Based on the internationally-recognized and community-developed CIS Benchmarks, a remediation kit takes those benchmark recommendations and puts them into Windows Group Policy Objects (GPOs) and shell scripts for *nix based systems (such as Unix or Linux). Available through CIS SecureSuite Membership, remediation kits provide another vector to distribute secure configurations though either the group policy management console within Windows or via a shell within the *nix environments.

Moving towards confirmed compliance

Remediation kits can implement secure configuration settings in just a few minutes; however, there is one caveat. Not all recommendations from a particular CIS Benchmark can be deployed in this manner. For example, EMET recommendations are not included within the Windows remediation kits, because it is an external download from Microsoft. Where the CIS Benchmarks provide recommendations and CIS-CAT Pro assesses for compliance, remediation kits provide the “glue” of assurance by implementing configurations.

To get started, organizations should first establish a benchmark requirement. Secure configuration requirements should be documented as part of the operational security standard. Next, deploy secure configurations – this can be a manual process, or it can be automated with remediation kits. Third, establish continued monitoring. Be sure to define how often you're going to review and assess configurations. The decision could be based on resources, but in most cases a recommended approach is to tier systems based criticality and risk. Tiering systems based on this categorization will define what should be scanned more often and those third- or fourth-tier systems that can be scanned less often.

For example, let's say Company A deploys CIS-CAT Pro to scan monthly on their critical infrastructure. CIS-CAT Pro will confirm compliance or may discover a configuration that is outside the Benchmark recommendations. Company A has two options:

1. Approve the change based on organizational needs and document a known deviation from the delivered Benchmark. As long as exceptions are documented, approved, and also referred to in the compliance check, Company A is still compliant.
2. Recognize that an unauthorized change has occurred and correct the configuration either manually or with a remediation kit.

Learn more and download a sample Remediation Kit

Keep Your Employees Interested in Cybersecurity Awareness Training with these Tips

As organizations work to make internal company processes and personnel more secure it's worth asking, "Are we doing enough?" Rehashing an annual awareness training or a yearly email phishing campaign may not be enough to thwart ever-evolving attacks and nefarious activity.

Get interactive!

To combat "training fatigue," which can lead to users not practicing what is preached as best controls, it makes sense to implement more interactive methods of cybersecurity policy awareness and training. These come in many forms:

- **Phishing campaigns**: Conducted by an internal "red team," internal phishing campaigns can train employees to spot and report suspicious emails they may receive.
- **Desktop/tabletop exercises**: These cybersecurity exercises help employees learn how they would handle an incident such as a DDoS attack or website defacement.
- **USB drops**: Are your employees trained to handle a mysteriously-found USB device? Find out with these exercises.

Be sure that these training methods aren't simply tested and then forgotten. Cybersecurity awareness comprises continual processes of integrating behavioral change into the business process. While technical controls can significantly improve security posture – implementing SPF, DKIM, or DMARC to reduce the risk of a successful phishing campaign, for example – it is important that the technical controls are not the only assessment performed against your organization. In addition to conducting training and awareness programs, managers should invest in understanding the analytics resulting from these programs.

Improving privacy and awareness

It's essential that organizations implement security in the form of role-based access controls (RBAC). Privacy, a key component of GDPR in particular, has become a highlighted requirement for organizations, especially those who manage and safeguard personally identifiable information (PII). Each industry (healthcare, finance, academia, etc.) maintains data that requires a form of protection. As this data becomes more integrated across business units and functions, knowing what types of data you're managing will allow specific training programs to be built.

Often, awareness training requires multiple approaches. For example, you might conduct a phishing exercise against a particular department or utilize a multi-email phishing approach for the whole organization. This can allow the organization to more authentically gauge clicks, versus the exercise-defeating murmurs of "Hey, don't click that!" which can spread through an office quickly. You'll also want to take into account different learning styles. For some, a PowerPoint may be enough; others might require a more hands-on approach to security training. A strong training program will comprise multiple approaches to cover a variety of training techniques and learning styles.

→ CIS Control 17: Implement a Security Awareness and Training Program

Additional Information

Resources

A list of all of the resources mentioned in this guide.

CIS Benchmarks: https://www.cisecurity.org/cis-benchmarks/

CIS Controls: https://www.cisecurity.org/controls/

CIS Cybersecurity Minute: Positive Effects of Patching: https://www.youtube.com/watch?v=Ls8frAIGP08

CIS Hardened Images: https://www.cisecurity.org/services/hardened-virtual-images/

CIS SecureSuite Membership: https://www.cisecurity.org/cis-securesuite/

CIS-CAT Lite: https://learn.cisecurity.org/cis-cat-landing-page

Sample Remediation Kit: https://learn.cisecurity.org/remediation-kits

Webinar: CIS-CAT Pro Demo: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-webinar/

Webinar: Where Privacy Meets Security: https://www.cisecurity.org/webinar/where-privacy-meets-security/

Whitepaper: Are You GDPR Ready?: https://learn.cisecurity.org/gdpr

About the Author

Sean Atkinson was named CIS’ Chief Information Security Officer in 2017. He uses his broad cybersecurity expertise to direct strategy, operations and policy to protect CIS’ enterprise of information assets. His job responsibilities include communications, applications and infrastructure.

Prior to CIS, Atkinson served from 2014 - 2017 as the Global IT Compliance Manager for GLOBALFOUNDRIES, a semiconductor foundry that manufactures integrated circuits. He led GLOBALFOUNDRIES Governance, Risk and Control management worldwide. Atkinson’s accomplishments included managing their compliance program to successfully combine multiple regulatory requirements into a single program of internal control, mapping into a Committee of Sponsoring Organizations’ Enterprise Risk Management framework.

Atkinson was the Internal Control Officer, Enterprise Risk Manager, and Information Security Manager for New York State’s Statewide Financial System

Program from 2007 - 2014. In this role, he was charged with policy, procedure development, and compliance with New York State Office of the State Comptroller security standards coupled with controls and risk analysis based on the National Institute of Standards and Technology's 800-53 best practice and audit recommendations.

Atkinson serves as an Adjunct Professor in Computer Science for Albany's College of Saint Rose. He earned a BS from Sheffield Hallam University, an MBA in Technology Management from Drexel University, and a MS in Computer Information Systems from the College of Saint Rose.

Atkinson's extensive cybersecurity credentials include a Certified Information System Security Professional designation and a SANS Global Information Assurance Certification as a Certified Incident Handler.

About CIS

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. Our CIS Hardened Images™ are virtual machine emulations preconfigured to provide secure, on-demand, and scalable computing environments in the cloud.

CIS is home to both the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to 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 cybersecurity needs of U.S. State, Local and Territorial elections offices.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061

518.266.3460

learn@cisecurity.org