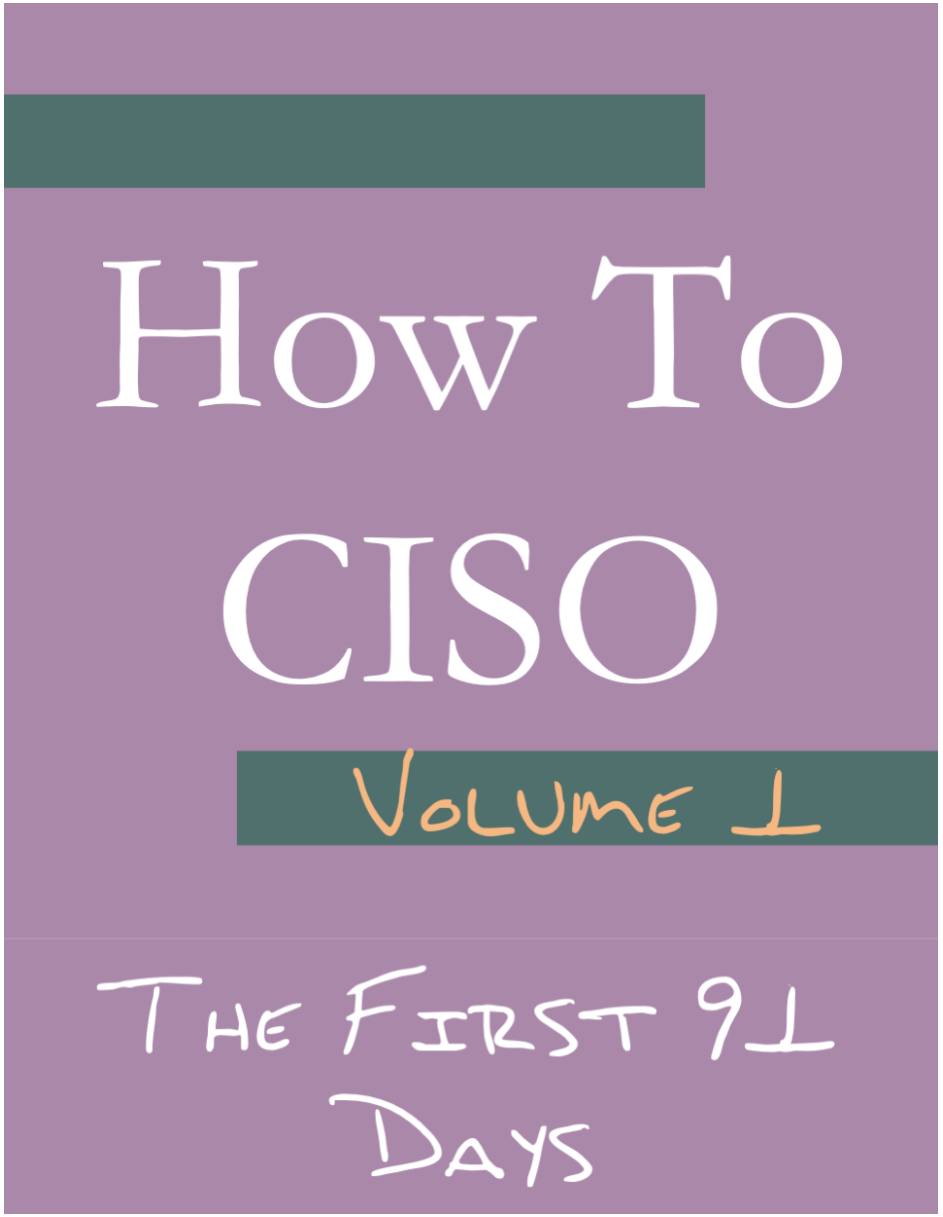

How To CISO
Volume 1
The First 91 Days

Version 1.1

By Andy Ellis

Introduction

Welcome to your new CISO gig! Whether you're a first-time CISO, or this is your tenth CISO gig, I've prepared this quick reference guide for you. Hopefully, it'll help you keep all your ducks in a row, balls in the air, and metaphors from mixing. This guide is high-level, with areas you should think about, and I'll try to stay out of the weeds on specific technical approaches.

Ninety days is generally the grace period (or "honeymoon," if you'd like) that a new executive has to get acclimated to a new environment. At the end of this time window, your employer is going to expect you to be executing on a plan, anyone you need to meet will expect you to have already made a connection, and any big changes in your plan will already need to be underway. This guide covers that first quarter – really, 91 days – with a primer on all the things you'll need to think about to get started with some early successes.

Using This Guide

As you start your new position, you're going to be juggling a lot of balls in the air as you try to learn your way around. Becoming familiar with your new environment isn't a linear process; rather, you're gathering information about people, organization structure, processes, tools, and risks all in parallel. This guide will help you think about what questions to ask to be familiar in each of those areas. Each section covers one theme of your onboarding, but you'll need to simultaneously approach all of the themes.

I'd recommend giving the entire guide a quick read-through, to get a feel for what you need to be doing in each area, so you can do them all at once – meeting people while assessing the security architecture to design the right plan going forward. At any given point in time, you're probably using this as a reference to make sure you don't miss important areas.

About the Author

Andy Ellis was inducted into the CSO Hall of Fame in 2021, so he should know something about being a CISO. He also wrote a book (*1% Leadership*), which has some small relevance in building teams and organizations. He is a Partner at YL Ventures, the Editor at How to CISO, and Principal at Duha.

Getting Ready to Start

Volume Zero ("The Idealized CISO") covered all of the different parts of the CISO role, so this guide starts with something you should understand before you start in that role: Understanding the organization that you've just landed in. If you haven't yet started, you can do a lot of this research from outside, and be a little ahead of the curve. But keep in mind that you'll want to keep testing your assumptions.

Understand Your Organization: Critical Questions

Every organization is different. Some organizations already have a strong adversarial relationship with their employees, and when you propose a bevy of tools that monitor employee behaviors, implement strong-but-slow processes to secure workflows, or limit usability to protect user data, no one will blink an eye. But when you apply those same suggestions to a more collegial organization, one which distributes power to its employees, you'll find you're met with obstacles at every turn. So your first step is to understand your company. Not just at the high level–you'll need to map out the entire organization, and understand what norms are different in different parts of the business. Most of this can happen in parallel with other work you'll be doing. Think of this as a mini-MBA specific to your company.

This section covers *what* you will want to know; the section on *Meet the People* covers *how* you might gather that information after you've started. You'll use this understanding to guide your interactions with your peers and stakeholders, and as input into building your security architecture. Each section covers a critical question that helps you distinguish your organization from others.

> *Goal: Define the nature of the business and how these constrain the CISO roles and responsibilities.*

Carbon or Silicon?

As you explore the parts of your company, look for the dominant paradigm: whether this organization is carbon-based or silicon-based. In a silicon-based organization, humans are generally *tolerated* as a necessary component of the business, but the primary value is found in the computers. Often the scale of the business is large enough that marginal costs need to be minimized to support a mass business model. Design patterns generally focus around eliminating human work altogether, and security is often oriented around eliminating insider threats. Call centers often fall into this category; the more operations are focused around "data in a system" and less "knowledge a human brings to the process," the more you're in a silicon-based organization. In a carbon-based organization, humans are generally the centerpiece of any process. You'll find a tension between IT processes, which, in many organizations, assume that the computers are important, and the users supported by IT, who see themselves as more important than the systems that they use.

In a carbon-based organization, you should heavily focus on the security user experience, because a bad user experience can capsize any initiative. In a silicon-based organization, you should focus a little more on measurable risk reduction.

> *Read more: Skynet or The Calculor.*

Immortals or Desperate for the Next Meal?

Most organizations have a hard time articulating their risk tolerance, but there is often a simple way to assess whether it is closer to zero, or to infinity: are you losing money (like a startup), or gaining money (like *most* established companies). If you're gaining money, then you probably operate similarly to an immortal. An immortal is generally risk averse; and avoids leaping into danger, especially for only minor benefits. Similarly, an established business has a lot to lose from major failures, so tends to move more slowly, trying to avoid obvious mistakes. A company desperate for its next meal, on the other hand, is always at risk of perishing. It has to move fast, and take high risks, just to get its next meal. Large amounts of danger are not at all threatening when you are already doomed to die.

If you're in a desperate organization, expect fast-moving, risk-taking behaviors, and a resistance to implementing safety processes that might slow things down; but expect more tolerance for implementing cutting-edge tools that might have imperfections. In an immortal organization, you'll find more acceptance for stable processes, but lower tolerance for unstable solutions.

Read more: Zombie Vivification

In Crisis, In Transition, or Stable?

Something caused your company to choose to hire a CISO. There are generally three different situations. One is that you're brought in to solve a crisis, often post-breach. Maybe you're their first CISO, and you're going to have quick wins. Maybe instead, the organization has a security program, and there was a CISO, but you've been brought in to transition the program to a different level of maturity or focus. Perhaps everything is going smoothly, security just works, and you're just coming in to continue running a great program.

It's important to understand where on that spectrum you are. An organization in crisis is going to be looking for quick, actionable, technical wins. One in transition probably expects to see you making structural organizational changes. And a stable organization wants to hear that you aren't blowing things up just for the sake of blowing them up.

Big Fish or Small Fry?

The size of your organization – both the InfoSec team and the overall company – are big drivers on the nature of your security program. A Fortune 100 company with multiple independent divisions may lean more heavily on governance and advice giving than a scrappy startup focused on getting to its first SOC report. You may be a team of one, expected to be deploying and running the security systems yourself; you could be leading a small group, focused on efficient execution and operations; or you could be running a large-scale organization, balancing risks across the business.
It's going to be important to not only know which size of organization you've inherited, but what expectations your stakeholders have for the type of organization you're going to build.

Lost in the Masses or a Magnet for Attention?

A lot of companies never seem to draw attention to themselves, while others seem to always be in the news. How you're going to approach security is going to be impacted by this; while some adversaries will attack anyone, others are going to be especially persistent if you either have some interesting asset, or perhaps you have a controversial business model or outspoken executive. Understanding why people might target you for extra attention, and what their specific goals are, might help design some specially targeted defenses.

Broad Governance or Tactical Execution?

Understand where your team fits inside the organization. If you sit near the executive suite, you probably have broad governance across the organization, with the ability to set (although not always enforce!) company policy. Your team might instead be embedded deep inside the organization, and your mandate is to simply execute on tactical security programs. Perhaps you're doing both, and you have to juggle both the execution of your policies *and* the evangelization of strategic initiatives in a broad way.

Success: Outcomes or Effort?

The value judgements of your organizational leadership – the principles that drive the organization, and how they understand excellence and accountability – should heavily affect your decision-making, as you'll want to leverage those organizational dynamics instead of fighting against their tide. If you can identify places where the organization is held back by a lack of (desired) excellence, those may be quicker wins than trying to apply excellence where it isn't desired.

Some organizations heavily value *effort* rather than *outcomes*, often because outcomes are harder to measure. Those organizations might be more appreciative of strategic work with qualitative improvements, with governance, process improvements, and shift-left business partnerships being higher on your priority list. Organizations that are outcome-driven might be more aligned with your overhaul of metrics, efficiency improvements inside your organization, and major projects that align with well-understood pain points.

Gaining Situational Awareness

The hardest part of being new to a company is how little knowledge you have about so many things. Learning, and learning *fast*, is going to be critical. You need to learn from the people in the organization, while you start to understand the business more deeply, the environment you operate in, and the critical players.

Know Yourself

It may seem odd to start a section about the situation you find yourself in by being self-reflective, but knowing how *you* operate best is critical context for how you're going to relate to the people around you and the organization you find yourself in. If you're better at strategy and alignment than at tracking details and driving work to conclusion, you'll be much more effective with a Project Manager or Chief of Staff to drive execution, and an Executive Assistant, even part time, will be a force multiplier on making sure you spend your focus on the projects that actually need your attention. Solving the things that make you the bottleneck in your organization may seem selfish–but it's really about making the whole organization more efficient.

Meeting People

You are going to need to meet a lot of people in this 90-day window. Everyone who works for you, your peers, the executive team, and, hopefully, the board. While technical skills might have gotten you hired, your people skills and your understanding of process are how you'll be judged.

You have a few goals in these conversations, and you need to balance all of them. You'll have some people who are excited about you joining the business, while some people are nervous. You want to channel that excitement while making sure you don't over-inflate expectations, and you want to assuage that nervousness. You also want to learn from the people who've been in the company for a while, to accelerate your own understanding of the company. You'll want to learn the cultural language of your organization, from definitions of terms like "Critical Risk" to understanding what phrases resonate – and which ones don't. You don't want to offend someone by lauding a program they've recently been burned by … or denigrating something that didn't work at your last organization, which everyone here loves. Finally, you want to set expectations for what you'll do once you're outside of the 91-day "honeymoon" window.

TYPE OF PERSON	YOU SHOULD	BUT DON'T
Excited	Channel excitement	Inflate expectations
Nervous	Calm concerns	Ignore worries
Long tenure	Learn history and culture	Accept "we've always done it this way"
Recent hires	Listen to ideas	Ignore side effects

Goal: Build rapport, establish trust, and gain inputs to assess the security program.

Your Team

You need to meet with everyone who works for you, in an either direct or indirect capacity, as quickly as possible. This should be a Week 1 goal. I recommend an All-Hands meeting to introduce yourself. Get yourself invited to every staff meeting of your sub teams (those can happen outside of Week 1, but make it a priority to get the scheduling worked out Week 1). Depending on the size of the team, figure out the

cadence for meeting as many of your team as you can individually. Even if this is an organization in crisis, and you're going to be making big changes, you will need to learn a bit about the organization. And you'll increase stability. Nothing signals, "We're all going to be let go" faster than not getting to even meet the new boss. Some possible important questions to ask:

- What does your team do? What valuable work am I unlikely to notice?
- What initiatives that the last CISO was driving were really valuable, that I should make sure I pay attention to?
- Conversely, what were they pushing that you didn't understand the value of, and I should look at to see if we can stop?
- What is the biggest gap in our organization? If we had a free headcount, where should I put it?
- What aren't we doing that it'd be embarrassing to explain that we weren't doing it?
- How do we measure success today? Is everyone aligned on these measures, or are there stakeholders who aren't on-board with them.
- What does our incident history look like, and what have we learned from them? How does that compare to our audit findings? What aren't we learning from as an organization?

Note that in all of these questions, you need to establish that you are trusting the information you are learning from your team. While you should maintain some skepticism – after all, humans are imperfect at describing the world – in your first encounters, your goal is to listen to everything they are willing to share with you. Even if you hear unbelievable things, this is not the time to tackle them.

Your Partners

Finance. HR. Legal. Facilities. All of those "General and Administrative" functions that executives tend to ignore until the last minute? Those can be your best allies in learning the organization, understanding how you'll get things done, and in avoiding the pitfalls of modern corporate culture. You'll want to build a strong relationship from the get-go, while also understanding that their priorities might not always line up with yours. You'll need to establish that you can work with these functions on their terms, so that when you need them to step up and support your initiatives, they're more likely to. The goal of these meetings is to learn how these organizations work, and how you're going to integrate with them to reduce friction in the future, while also identifying places that

- Finance: What's in your budget, and how is it defined? What does the annual budget cycle look like? How does new budget get allocated, especially if a peer organization asks you to do new work? If you discover a need, what will that process look like? How is Finance today protecting itself from attacks aimed at redirecting money transfers?
- HR: How does your HR team engage with your managers on personnel development? What is the hiring process, and how are you ensuring you get great candidates? What bandwidth do they have for organizational development, and what experience do they have with it? What does staff turnover look like in your organization, and can you read the exit interviews? How is HR dealing with the influx of fraudulent applicants?
- Legal: How do you share responsibility for various types of compliance? Is Legal tracking impending legislation and regulations around cybersecurity and privacy, and how do you tap into that? What standards for vendor management does legal enforce, and how can you plug into that process (as a buyer or as a vendor)?
- Facilities: Who secures your buildings, and how does the access control system function? Is the Facilities team using security data (badge-in records) to also manage space allocation, and how might that create perverse incentives for employees?

Your Peers

While it's important to have stability with your team, your peers are the people who ultimately will make or break your career (or at least, this piece of it). Your conversations with them ultimately have the goal of them becoming champions of your security program … which is best achieved by giving them a hand in developing your program. For them, you have a different set of questions. I'll put the two most important questions first, but you should weave them into your conversation, not lead with them. These questions are important because they'll give you a list of candidate changes to make quickly, that will earn you political capital across the organization.

- What is a security practice that we are doing, that is high cost and low value, that you think we should stop?
- What is a security practice that we aren't doing, that you think we obviously should be doing?
- How does your organization provide value to the company? How do you measure your team's success?
- How can my team help? Are we doing that today?
- How often does security come up on your radar?
- When you last briefed the executive team, what was it about? Can I get a copy of your slide deck? And if you have one on your overall roadmap, can I get that too?

Your Customers

While you might want to wait until you know more about your products and services before you go talk to customers, in your first few months you have an opportunity to build relationships with key customers, and learn their painpoints, while at the same time building good will with your Sales organization. Ask to meet with a handful of customers, especially customers who've historically wanted to engage around security. You can also meet with some marquee customers who don't currently have executive sponsors. Reach out to your professional friends who are CISOs at your customers as well. The goal of these conversations is to understand the stories behind the metrics around customer loyalty and pain, and to determine if there are customer drivers that align with your security program.

- Why do you buy our services? What is our differentiator against our competitors?
- How do you think about the risk of using any vendors, and us in particular? Are there any pain points that could be improved?
- Are there features you've been looking for that we haven't delivered? What have you been told about why?
- Have there been any incidents that adversely affected you? What did communication look like?

Your Executives

Odds are, you met with many of the executives during the hiring process, but you'll need to meet with all of them again. Your first pass is "your boss's peers," which might be the same as "the CEO's direct reports." If it isn't, add in the CEO's direct reports to your second pass; if not, include the CEO as your second pass. The goal of the meeting with them is to set expectations for what you're doing, and when they should expect to see a readout from you. These meetings should be relatively brief, as you're mostly just getting your face in front of them. A few key questions to ask:

- After I finish my 90-day assessment, and bring my roadmap around for review, what will you be looking for?
- Do you have any advice based on other new executives' successes and failures?
- Can you give me insight into how the board, and other executives, operate?

Tip: Remind your executive stakeholders that if you're doing your job well, you'll keep discovering new problems even outside your first 91 days, but that's to be expected.

Your Board

Before you meet with the board, you're going to need to learn who they are. Often, there is someone, usually in Legal, who has the unofficial title of "Board Handler." Actually, two of them. One is the General Counsel's Executive Assistant, and you should make friends with them very quickly. They'll be able to tell you all about the personalities of various board members, as well as connect you to them. The other is often an Associate General Counsel, and they'll be able to brief you on the interactions of the various board members inside the boardroom. It will probably take you a while to set up meetings with the board members, but you first need to identify which subcommittee you'll be reporting to (some CISOs will brief the whole board, but many report to the Audit Committee). You'll want to find out which board members are knowledgeable about cybersecurity and technology, and which ones are engaging on the topics (these might not be a perfect overlap). See if you can schedule some introductory meetings with the interested board members. Some topics to ask them:

- Do you have any other companies that you really like the way they report to the board? Can you introduce me to their CISOs?
- What has been lacking in the previous board conversations around cybersecurity?
- What in previous board reports did you find most valuable?

TIP: Identify all of the other companies that each board member is affiliated with, and search for those companies' cybersecurity events – a breach at one company a board member sits on will often result in them asking targeted questions about your security against that same type of attack.

Learn Your Environment

Every time you hear a statement about your security program, you need to ask which systems are in scope. You need to identify where the gaps are that everyone has forgotten about, because they only think about risks to the assets that *they* think they are responsible for. This is where you start to shine a light into shadow IT; as you pay attention to security gaps for systems that aren't well supported.

Goal: Understand the scope for your security program.

Unacceptable Losses

While it may be tempting to jump right into Asset Discovery, you need to inform your view by understanding what are the harms that your company most worries about. Perhaps you ask every stakeholder "What does the worst day for our company look like to you? What would make it the worst day?" Consider who relies on and uses your products and services. Think about how your company could (hopefully inadvertently) harm them.

Example: in the airline industry, assets might include planes, systems, and gate reservations. Unacceptable losses are more likely to cluster around harm to passengers. While that harm might come from the assets (planes crashing, systems exposing sensitive information, error in gate navigation causing missed flights), those losses don't always become obvious when only looking at the assets.

Assets

My favorite asset management tool is a spreadsheet. Not one to count systems, but to count *types* of systems – your company probably has one or more asset management systems to track specific systems. In your spreadsheet, not only will you list the classes of assets that are tracked (laptops, servers, routers, etc), ask what types of systems *aren't* tracked in inventory management, and add those categories to your spreadsheet.

Some types of systems you might want to consider looking for on your list:

- Enterprise (supporting your employees and corporate entity)
    - Laptops, Desktops, VMs, Servers (and see if Windows tracked separately from Linux), Active Directory domains, routing infrastructure, IOT (Room schedulers, cameras, badge readers, elevator controllers, HVAC, white noise generators). See also Cloud and SaaS below.
- Production (If you have a product that you sell)
    - Development Labs, QA, Build System, SDLC infrastructure, Production servers, databases. Code signing infrastructure, auto-updates might also be relevant. See also Cloud below.
- Data Centers (if you manage any)
- Cloud
    - "Multi-cloud" often means each development organization chooses which cloud service providers it uses. Often, you may find that even systems in the same cloud provider are managed under entirely separate administrative accounts – the easiest way to get a full inventory may be to check with your Accounts Payable team in Finance to identify where the cloud spend actually is.
- Internet Glue
    - You may have your own autonomous system (AS) for routing. You probably have DNS domains. Identify who tracks and manages these – and understand where there may be systems managed externally – marketing microsites on continents away from your headquarters are a good place to look.

Data

While most people think about *systems* as your important asset, for many organizations, it's the data that is your crown jewel. In non-cloud environments, large datastores can often be found by looking for your systems with large storage clusters. But not all data is stored in massive storage clusters, and in the cloud, data might be proliferating in surprising places. Some of the data you hold may be regulated, and some may just be sensitive for your business. Understanding your valuable data is key to protecting it.

Find out what data your organization keeps, and where it is stored. Some of it is in datastores that you manage, other data is in SaaS applications, and third parties probably maintain even more. While most organizations correctly remember that if you have end users, their data is important, don't forget to assess your employee records, information about your customers, and any data you may be getting from third parties.

SaaS

Software-as-a-Service (SaaS) has increasingly become a dominant paradigm for businesses. While a decade ago, most SaaS applications were IT-owned standalone services for back-office applications, SaaS-native ecosystems now abound. Companies empower business users to adopt SaaS applications in every business unit, from R&D, marketing, sales to HR, creating a convoluted web of SaaS applications, data flows, identities and third-party integrations.

Learn what your SaaS ecosystem looks like. Identify the many SaaS vendors your company relies on (It's probably much larger than anyone thinks). Identify which ones are configured to use your single-sign-on. Find all the third-parties that access your business critical SaaS data. Check on the deprovisioning process. Understand which users have administrative access to reconfigure your core SaaS apps.

Use what your company uses! Maybe you're a diehard Google Workspace and Zoom user, and you've come into a shop that's exclusively Microsoft. Start using Office365 and Teams for everything you can. Become a power user of the same applications that your company uses, and don't look down on your peers for using different products than you do … instead, become the helpful and friendly advisor on how to best use the tools in your ecosystem.

Learn more: How To CISO Handbook: Environments

AI

Artificial Intelligence in its many flavors (data science, machine learning, NLP, process automation, generative AI, LLMs) is already embedded across your ecosystem. The rise of applications like ChatGPT made AI more approachable to your organization, because for the first time integrating AI into an employee's workflow could happen with a few simple sentences, rather than requiring developer-years of effort to integrate it into tooling.

Think about how you're using AI across your environment. Your products may have AI embedded behind the scenes, or might include helpful agents to interact with customers. Your SaaS tools almost certainly have AI threaded throughout their architectures. Your customers might even be using AI to interact with you as a vendor.

As you evaluate AI use in your business, pay attention to where major changes will be acceptable, and to where efficiency and productivity drivers are going to override what might feel like academic concerns.

Learn Your Product

Hopefully, you're in a business that delivers some form of goods or services, profitably (or, intentionally non-profitably). Understanding the business value chain is doubly important for your success. On one hand, being able to describe security projects in language similar to that used for the business will be helpful in being seen as a business enabler. On the other hand, different business models have very different security issues, which you should make sure you're thinking about.

You'll want to understand not just the transactional part of your business (where money is exchanged for goods/services), but the entire business process that leads to that point – and beyond. That may encompass customer acquisition, product development, supply chain, service delivery, customer support, and numerous other business functions. Looking at an organization chart, and asking how each part of the company supports the delivery of value to the customer may tease out business processes that you weren't aware of … but still need to protect. If the business is sufficiently novel to you, see if you can take time to work in parts of the business – even a few hours on a manufacturing floor or behind a cash register can give you the right perspective for your new organization.

While every business still has a core enterprise IT function, and information security needs look similar even between disparate businesses (every organization needs to keep end-user systems up to date!), your business model will often drive very different product security needs. A few notable examples are below, feel free to skip the parts that aren't actually relevant to your business.

Goal: Learn the unique elements of your business and how it makes money. Learn the language of the business to better communicate with your stakeholders.

Physical Goods

If your business produces physical goods (automobiles, consumer packaged goods, etc), you may not have a separate IT program to support the product side of the house, and product information security is going to be embedded into enterprise information security. Likely, one of your biggest risk areas is around *product designs*, especially if your manufacturing arm is outsourced.
Supply chain management in your company is likely focused on safety and resilience of your suppliers and shippers. Security vendors who talk about the "supply chain" generally are focused on the *software supply chain*, so be prepared for some confusion as people reuse language. There are some subsets of physical goods, however, that may have their own IT (and thus information security) challenges.

Manufacturing

Your company makes things. You might also sell them to consumers, or you might be deep in the supply chain. Internet of Things (IoT) is probably a huge area you're going to need to pay attention to, as well as Industrial Control Systems (ICS). Securing the interfaces between your corporate facilities and your manufacturing systems, especially against ransomware, probably needs to be fairly high up on your radar.

Hardware

Maybe your company produces electronic hardware. Firmware updates are definitely an interesting problem. Your supply chain security problems are more durable, since you can't just replace your entire install base in the way a software supplier can. Your company might make disposable hardware, where you don't support it for long, or produce capital goods, with supported life spans measured in decades. You may have a revenue stream from supporting hardware in the consumer's hands.

Customer-Focused Services

Your industry might be focused on delivering personalized and tailored services to individuals, and you're entangled in their PII as part of delivery. You may have specific security hazards as part of your specific model, but protecting the core record about your customer – and the details about what you do for them – will usually be the primary driver for your security program. Privacy is a significant concern for you, and understanding whether you own privacy, or you're partnering with another organization, will inform how you move forward on protections that implicate both privacy and security.

Healthcare

If your business is a large healthcare organization, you likely have to deal with more transient staff than most businesses, and those transient staff often have significant access privileges. At the same time, many of your customers might also be temporary, and some of them might be celebrities – and the details of their use of your service are financially interesting to adversaries.
While confidentiality is likely paramount for you, managing availability is also a life-safety issue, and you likely have tensions around connected-but-neglected clinical devices.

Financial Services

Your customers have placed significant trust in you – while their privacy matters a lot, control of their money requires significant protection. In some cases, your adversary might live in the same house as your customer, and you'll need to consider how you protect your customer not just against random account takeover, but from hostile family members as well.

Education

Your customers may also be your tenants. Students may have a complicated relationship with you, and your IT systems. Like healthcare, with its transient doctors, you may have transient lecturers. You also may have research labs and schools within that barely tolerate having centralized IT, and not at all centralized security governance. You may need to operate much more with influence than authority.

Software

Instead of physical goods, perhaps your company produces *software*. You may operate your software as a service you sell (SaaS), or you might distribute the software. Those models have different ways that you'll need to deal with bugs and updating your software in the field; you may also have very different threat models. Your software supply chain becomes front and center; but unlike the physical world, where you're paying attention to the logistics of delivery, you're probably more focused on the provenance of the contents.

Packaged software

If you package software for sale or licensure, you have different constraints on how you can fix defects (security or otherwise) post-deployment. Since you don't have control of systems running your software, you'll need to understand how updates happen. Whether or not you provide an automatic update infrastructure, you'll need to assure the integrity of the updates to your customer. But in an automated update system, how you control updates, detect errors in the fleet, and provide rapid response becomes more critical.

If your business enforces software licenses, understand how the licensing system works, and how you may be introducing significant dependencies to your customers.

Software as a service (SaaS)

If you operate the software that you make, defect fixing is usually an easier problem, but *customer isolation* needs to be at the forefront of

your product safety team's mind. You'll likely also have to address how your employees gain access to customer data and operating environments. Customer support teams often require on-demand access to customer sites, and broad access permissions can create unpleasant risks for your organization.

Professional Services

If you're billing hours – or even just bundling support services into your contracts – the access control for your staff who manage customers becomes a key area to address. You may support third party managed service providers and your channel partners, who want to provide professional services on top of your services.

Retail

If you're directly selling goods to end users, online or in stores, you probably also have to pay attention to fraud (whether that's a different organization or not, you'll be overlapping in a lot of places for data collection). With physical locations, the relationship you have with the physical security team is a lot more important. How you support point of sale devices becomes interesting – both payment processing terminals and checkout devices.

The State of Security

If you understand your environment, you can evaluate the security controls in place around it against the attacks that you're likely to encounter. Your environment is likely highly complex, and you'll need to approach it from a number of angles before you can find the hidden deficiencies. The next few subsections should help you understand all of those angles: the attacks you are at risk from, the vendors and solutions you already have, the functions in your security organization, and the capabilities you need. You'll then be ready to identify the changes you'll want to start making.

TIP: Map your security program onto the Cyber Defense Matrix by Sounil Yu. It has similarities to the NIST Cyber Security Framework, making for ready portability in the event you have a stakeholder that wants to see your program laid out against the NIST CSF.

Map The Attacks

As you learn more and more about your environment, you should evaluate how resilient it might be against attacks, from common to esoteric. You should understand how common, well-known attack types (e.g. ransomware, phishing, business email compromise, account takeover, DDoS) might operate in your environment. You should also learn how your own services might expose your customers to attack, and how many of those are exploitable under the default configuration choices you give your customers, versus which might require software defects to expose.

As you're doing your initial learning conversations, understand if any of these attacks have recently affected your company. Ask for stories of past incidents, and understand how the company reacted to those.

Goal: Articulate risks to your business in clear, broad language to communicate across all stakeholders.

Common Attacks

Build an attack path narrative for each common attack. At this stage, these should be very generic statements, which ignore your current controls, but usable to simply describe an attack in broad terms to one of your partners. A key part of these narratives is that you can decompose the attack into a number of steps on the attacker's path, and you'll later assess your security controls to see if they mitigate the hazards that make those steps easy or possible. Some of these narratives are composable into larger attacks, for instance, an attacker might use *phishing* to engage in *account takeover* to then begin a *ransomware* campaign. Here are a few narratives to get you started.

TIP: Make these narratives basic and simple. Much like fairy tales, they serve as cautionary warnings, not complete blow-by-blow analysis of every defect. Ease of communication is more important than having a perfect description.

Ransomware: An adversary gets malware to run on a machine by any number of methods (phishing, account takeover). That malware moves laterally by exploiting credentials available on that system (or exploiting known vulnerabilities accessible via network attacks), propagating across our environment, and stealing the data it finds, while leaving behind an encrypted copy. The adversary may offer to sell us the decryption key to recover. [Hazards: ability to run malware, administrative credentials that allow wide lateral movement, unpatched vulnerabilities on systems, lack of data backup/recovery strategy]

Phishing: An adversary sends a message to an employee that purports to be a legitimate instruction from the company or a trusted third party. The adversary is usually trying to get the employee to do one of three things: open an attachment/link that contains a vulnerability exploit for the application that will process the file, install a piece of malware directly on the system, or go to a website and enter their authentication credentials for the adversary's use. [Hazards: ability to send malicious messages to employees, employee requirements to interact with email, ability to install malware, unpatched client applications, reusable authentication credentials]

Business Email Compromise (BEC): BEC is adjacent to phishing, in that it usually begins with an initial message to a user, although that message might also be SMS or a phone call. The adversary generally pretends to be an executive or a partner, and requests the targeted employee to initiate a business process, like transferring funds. [Hazards: unauthenticated/easily spoofed email, business process without strong two-person controls]

Account Takeover: A legitimate user's login credentials are exposed to an adversary, potentially through a data breach elsewhere (reused password), a proxy attack (via phishing), or via a system compromise. The adversary then uses credentials to login to the user's account to conduct nefarious activity (install malware as an administrator, buy gift cards on a stored credit card, gather intelligence to conduct identity fraud). [Hazards: authentication that uses reusable secrets (passwords, PINs), lack of activity monitoring to detect fraud/suspicious login events]

Distributed Denial of Service (DDoS): An adversary with the ability to generate large volumes of internet traffic sends that traffic at critical Internet-facing systems. That traffic may overwhelm your network capacity, or may require expensive application processing to handle. Your critical applications become unavailable to your users. [Hazards: insufficient capacity, inability to prioritize legitimate traffic over attack traffic]

Industry-targeted attacks

Now that you've considered the common attack paths that any company could suffer, consider whether there are more specific attacks that are relevant to your industry. Maybe these are derivatives of common attack paths (for instance, *account takeover* can be used to perpetrate even more interesting attacks when targeted against customer support employees). You are trying to get a handle on the types of attacks that you and your competitors all need to worry about. Some prompts that might help tease these out:

- What specific third parties do you rely on for critical services? If those critical services are compromised, how does that affect not only your business, but that of your customers?
- Do entire industries rely on you and your competitors as service providers? How could an adversary harm your customers by harming you?
- If one of your employees went completely rogue, with no concern for the consequences to themselves, how could they abuse their privileges to inflict the most harm? What information do they have access to that could give them even greater privilege? (Note that you aren't strictly trying to identify insider threats; you are more worried about adversaries taking over your employee's access or systems)

Company-specific Attacks

Finally, you need to start understanding the various ways that attacks specific to your company can create a problem for you. These are usually the outcome of specific design choices or implementation details you might have inherited, and are often hard to easily identify. On the bright side, almost everyone in your company knows at least

one of these, and often all you need to do is ask. Some prompts that may help:

- What configuration options should our customers use, but most of them don't? Why?
- Who, if they left the company tomorrow, would create the most harm for us? Why? Is it related to systems they support, processes only they understand, or knowledge unique to them?
- What is our most fragile system?
- Where do we have the most technical debt? (NB: I'm not a fan of the term "technical debt", because debt is rarely compelling to business stakeholders, but "deferred risk" is. But in this context, it may be the easiest way to tease out a quick answer)

Learn Your Vendors

Odds are, you have a number of vendors who provide security services or tools to your team. And, now that you've posted on LinkedIn that you've started a new position, even more of them will be coming out of the woodwork. Before you can tackle new vendors, you should get a handle on your existing ones.

Your Finance partner or the Procurement team can often give you a list of which vendors are charged to your budgets. While you're talking to them, learn about the procurement process, and what hoops you should most pay attention to if you want to quickly acquire technologies or services. As you have these conversations, look at the renewal cycle for your existing vendors. There's a large difference in how you'll deal with a vendor with three years left on the contract, and how you'll deal with the urgency of a pending renewal. For ongoing contracts, verify that you have the renewal costs correctly budgeted in future years.

Goal: Understand what security needs you currently have covered, and what the limitations are of your security systems.

Integrators / Managed Providers

You may have vendors that either manage security solutions for you, or who provide value added services to other product acquisitions. You should get time with them very quickly, especially the technical architects, solutions engineers, or operators who interact with your company on a regular basis. Ask them the same questions you would ask your team. Learn what problems they are solving for you, and which ones they think you should solve next. Ask them about the efficacy of your current solutions ("If we turned off product X, would we even notice?"). They'll often help you identify what products were never well integrated, and that can feed into your plans for what to do next.

Platforms

Some of your vendors might be large platforms that provide you a multitude of services. Getting a briefing – perhaps asking to see the previous Quarterly Business Review – will be helpful in addressing many of the same questions you asked your integrators. But often a more insightful question is "What are we paying for but not using?" While some vendors may worry that this is aimed to start price negotiations (and it can be), you often have quick, cheap wins available to you by taking advantage of capabilities that your predecessor didn't. You should probably ask someone *why* those capabilities were never leveraged, just to make sure the vendor isn't downplaying the complexity of integration.

Point Products

Throughout your environment you'll also find point solutions, aimed at solving specific problems. Usually, point products are installed when you don't have another option, but over time, other choices might become more interesting. Look at how long point solutions have been installed, with an eye toward seeing if those systems are still providing value, or if they were installed and forgotten. Maybe you now have a platform that includes this capability, or there is an upgrade to a more recent version. In your first 90 days, ripping out a point product is rarely a good use of your time, unless it is causing significant business friction, is ineffective, or has a high support cost for your team. But a point solution that checks all three boxes might be the quick win you're looking for.

Auditors/Assessors

Your security program might have both auditors (vendors who certify your compliance against a standard) and assessors (vendors who find specific gaps in your programs). You should understand which of your vendors fall into which category, because you generally pay auditors

to give you a passing grade (so your employees rarely tell them where the skeletons are buried), but you pay assessors to give you a failing grade (so your employees love telling them what's wrong). Make sure you dig deep into your assessors' knowledge if you can.

In-house

You may also build security services and solutions internally. Your team can probably point you to these, but you should understand what they are, and how your team supports these services. Nothing is more embarrassing than deciding that certain people can be let go, only to discover that the last person who supported a critical service that all of your products relied on just left.

Cyber Insurance / D&O

It's important to understand what your company's strategy is for cyber insurance. Not only who carries it, and what coverages it has – but what might trigger your company to make a claim against it. What are your responsibilities when renewal comes up – maybe you'll be briefing the adjusters.

> *TIP: Check the company's Directors & Officers (D&O) insurance. If the CISO (you) are making Sarbanes-Oxley declaration, then insist that you are also named in the D&O policy.*

Assess Your Program

By now, you understand your company's environment, what risks it faces, and how your security program addresses those risks. And now you need to start assessing the gaps in that program. The more specific a gap can be, the better; the vagueness of a finding like "Security is not baked into the software development lifecycle" isn't going to be as helpful in communication as "Engineering teams X,Y,Z do not have security testing as part of their quality assurance program."

One way to find gaps is to take a control assertion someone makes ("We patch critical vulnerabilities, on average, within 7 days") and ask questions to identify gaps in that statement:

- What systems are in scope for that metric?
- What applications on those systems are in scope (how do you learn about vulnerabilities)?
- If the average is 7 days, what are the outliers? What percentage of vulnerabilities take longer than twice that?
- How is "critical" defined? What important vulnerabilities aren't deemed critical?
- How are exceptions measured? If a vulnerability is never patched, how does it affect the metric?

In addition to your own assessment of your program, you will also need to create a way to share that assessment. Often, this is the beginning of your ongoing Board report, but for now, you'll use it to communicate with your stakeholders.

> *Goal: Understand the gaps in your security program, and create clear ways to communicate those gaps.*

Through an Organizational Lens

As you assess your program, one axis to evaluate it on is *organizational*: exploring how risks tend to congregate, and comparing that to the teams that manage broad categories of risk. Some of the teams will align to asset classes – your Enterprise Security team generally tackles risks that line up to the systems that the Enterprise IT team supports – while other teams have a more functional mandate – a Security Education team probably focuses almost exclusively on training and branding activities.

Enterprise IT

This area might feel like the most cookie-cutter – every company has IT woes – but often it's the place where most attack paths progress. Make sure that your controls work as advertised here (your MFA might be really good, or it could be implemented with gaps that an adversary could exploit). Does IT have a good relationship with teams that deploy *Shadow IT* (IT programs supported outside IT). Understand who handles end-user security, and how end-users feel about that interface – this is often an area where there is low-hanging fruit for improvement.

Compliance

Compliance is, most often, a *product management* requirement, not a security requirement, but most organizations treat the security team, if they drive the compliance program, as if the security organization is the source of the requirements. Here in the assessment phase, and going forward, is your opportunity to clearly establish that you are a product manager, working for the main product managers in the organization. For everything you sell to your customers, understand the regulations and certifications required by each of the industry verticals that you sell to. You may not be a healthcare provider, but selling to them requires you to engage with HIPAA. Selling to the US Government requires FedRAMP. The list of compliance requirements worldwide is significant, but every one of them is a *product feature*. Map out which programs are required by which products, in consultation with the product management and sales organizations, and compare that against which controls you don't yet satisfy.

Product Safety, AppSec, and the Software Development Life Cycle (SDLC)

Product safety, across engineering, operations, and customer support, is the place that you'll most need to engage in careful communications. Gaps in your security program will rarely feel urgent to stakeholders, and often this is the place where you'll find the most deferred risk. Look for gaps that your partners identified for you as opportunities to get quick wins.

While the Product Safety team often sits squarely inside a broader Security team, the SDLC security program may be shared across many entities. SDLC security often includes integrity of the software supply chain (making sure that your software is not altered), third party software management (tracking and remediating known defects), and securing in-house developed code (often through security testing, developer education, and code refactoring). A bug bounty program might be an external validation and discovery tool on your in-house AppSec program.

Security Operations/Incident Response

When an alert fires, *someone* is responding. You'll need to identify who that is in the organization, and understand how they handle and process that information. For day-to-day issues – alerts fired by your tools, for instance – trace the remediation process, and see if the operations temp of the operations team matches the cadence at which remediation teams operate (a major mismatch in many organizations is an alert-driven ops team trying to drive work into a project-based engineering team).

Learn what your response program looks like for major incidents and breaches. Ensure your Incident Response plan includes both forensics aspects, as well as integration with your Communications team.

Look into how your organization learns from incidents. Find out the last few major incidents, and look into the post-incident report to identify the lessons learned. Understand why unresolved lessons are still outstanding.

Threat Intelligence

Understand how your team keeps abreast of the changing threat landscape. It might be you, paying attention to Twitter and LinkedIn, and hoping for the best. Perhaps you have a more systematic approach to learning about adversaries and adjusting your program. This will feed into your attack mapping program to keep it up to date.

Internal Education

Most companies rely on their users at some point as a last ditch line of defense for security. While you should focus most on removing that reliance – making it safer for your users to operate – you should still determine if you have the right education programs in place to help your users identify when they are under attack.

Human Resources (HR)

HR holds almost all of your employee data, but, more importantly, they're generally the start point for two of the most important security processes in your company: onboarding and offboarding. You often have some quick wins in cleaning up security issues around these processes, but you should make sure that some specific topics are securely addressed: provisioning of employee systems and authenticators, contractor (especially "passive overboarding," where their hours are dropped to zero but they aren't terminated), authorization to SaaS applications (and de-authorization), training in security norm.

Risk Register

Risk registers aren't just where risks go to die … although that can often be a very real risk. But if you can dig up a copy of every risk register, you can often find some very specific and pointed risks that you might want to know about. For any risk register that is active, you'll want to understand the *success criteria* for each risk. Knowing what needs to become true to remove the risk from the register will enable you to drive more actionable programs; and mandating success criteria as a part of risk registration will also clean up your ingest process.

Through a Capability Lens

Another way to assess your security program is to look at any given part of the program through a *capability* lens. There are a set of universal activities that span across almost any part of a security program. While a given implementation might use product-specific nomenclature (Cloud Security Posture Management is Configuration Hygiene applied on your cloud service providers), these areas will allow you to quickly verify that you have robust security programs across the board. Often, you'll need solutions that span multiple capabilities – a great Access Control system should have capabilities in Identity and Privileges, Attack Detection, Breach Detection, and Process Management.

Identity and Privileges

When a user (or automated process) tries to access a system or function, this lens covers how you decide if they should be allowed to do so. Important components are usually *Identity* (who your entities are), *Authentication* (how you prove who they are), *Authorization* (checking that they are allowed to do an action), *Entitlements Management* (giving and removing entitlements). Single Sign-On (SSO) systems generally allow you to centralize identification, authorization, and broad revocation (upon termination), so a first step is always understanding where SSO is implemented. Some systems may require federation with other organizations, and you'll need to assess how your partners are managing Identity.
Entitlements Management is an area where many organizations rely on manual, ad hoc workflows: help desk tickets, manual audits of grants. Automation capabilities for provisioning and deprovisioning are important at simplifying the user experience, while role-based

entitlements will reduce the confusion that often arises from the accretion of individual entitlement grants.

> *TIP: Walk through the workflow of an employee changing their name. Not just their display name, but their username. Systems that handle Identity and Privileges poorly will create pain for the user, functionally requiring them to behave as if they were terminated and hired as a new employee, rather than having their existing entitlements accept the change.*

Configuration Hygiene

Every system you have – whether it is a business or security tool – relies on being correctly configured and maintained. Rarely do systems have the default settings that meet your needs, so you need to make sure you have the capability to identify defects in configuration and correct them. This can range in complexity from very simple activities like disabling features, to fairly complex settings and interactions between different components. The various *Security Posture Management* systems, for Endpoints, Clouds, and Applications all fall into this category.
Understand whether a Configuration Hygiene system is a *detective* control (it just tells you there is a problem), a *preventative* control (problems aren't allowed to be deployed), or a *reactive* control (problems are automatically remediated). Your security program's Process Management capabilities are often critical to the success of Configuration Hygiene systems.

Attack Detection

The most common sorts of detective security controls are those which monitor requests or communications for malicious effects *before* they take effect. *Web Application Firewalls*, *Fraud Detection*, *Email Security,* and *Endpoint Prevention* tools often sit in this category. As with Configuration Hygiene, Attack Detection can be preventative or detective, and understanding whether your systems are denying traffic, or just alerting on attacks is important. Some Attack Detection systems are layered. Make sure that your program doesn't overreact to detected attacks that are seen *before* encountering an effective control that blocks them.

Breach Detection

When something goes wrong, your systems need to detect the error. Maybe there are artifacts left on a system after a breach, or perhaps a system notices behavior outside the norm. Anomaly Detection capabilities are centered on detecting *successful* attacks. Many security programs focus primarily on detecting and stopping attacks before they succeed; but every system should generally also be monitored for evidence that an attack bypassed other defenses and is now causing harm. The more a security program can block common attack vectors, the less your Breach Detection systems will be noisy with real-but-common breaches, and the more you can focus on detecting serious breaches.

> *TIP: When assessing your Breach Detection capabilities, take each system in scope, and ask, "If an adversary compromised this machine, what would they do then? Exfiltrate data, alter data, move laterally? How would we detect those steps?"*

Verification and Testing

Knowing whether or not your security controls are effective is a necessary part of your security program – probably always the next most important thing (right after you implement any security system, you should add a *Verification* system that makes sure it works). *Testing* systems are often similar to verification systems, but based on a different assumption – that you know that you have an imperfect security system. You want to find the places to quickly repair, while setting up programs that will sustain your improvements in the long run. *Penetration Testing* and *Application Security Testing* are two common systems you'll look for, but many verification systems tend to

be custom-implemented in organizations to keep track of existing controls. GRC teams are often the biggest users of verification systems.

Knowledge Collection

Security teams learn a lot of information – and keeping track of it is critical to making wise risk choices. *Asset Management* is core to keeping track of where your systems are, but a good *GRC* system that tracks all of your controls may make your learning curve a little easier to handle. *Incident Response* systems may help track your systemic risks. Understand how your security program takes advantage of the institutional knowledge your organization has collected over time, and how well it is curated. Data analysis across your knowledge management systems may be a source of interesting insights.

Process Management

Outside of quick fixes, a lot of security improvements come through robust processes. Some organizations rely on human project managers for most process management, and support them with various knowledge and tracking tools. *Orchestration* systems are usually helpful in specific process management areas, whether it is *Vulnerability Remediation* or *Incident Response*.
Automated systems will amplify your Process Management capabilities. Organizations can sometimes be hesitant around complete process automation, fearing chaos when an automated system does not detect an incipient or occurring failure. A lesson from operating trains may be useful here: most trains are driven almost completely by automation, while a human has a manual control to stop the train (and sometimes to speed it up or slow it down). Following a path to automation that leaves humans in broad control while allowing most of your processes to be run by automation can be a source of significant efficiencies.

Making Changes

Decide on Your Initiatives

Projects

You have a lot of good work in front of you. To help you prioritize, you should probably categorize your gaps into five categories, from worst to best: you're doing something but it is bad, you're not doing anything, you're doing the minimal, you're doing okay, and you're doing great. The more a project addresses gaps in the first two categories, the more you should consider those to be priorities. You can't afford to start boiling the ocean and solving all problems, so you should prioritize areas where you're getting a large improvement by doing anything at all, rather than investing too much of your not-yet-existent political capital on making expensive, marginal improvements in security projects.

Quick Wins

No one survives a long time in a company without building up political capital. Even if there is a compelling event that spurred the company to hire you, they still want to see you successfully execute. And the more you succeed, the more you *can* succeed. The more you fail, the more you teach your peers that they can let you fail. This category is for quick, easy wins; often the very projects that your peers suggested in your initial meetings. As you come up with ideas, prioritize them based on how non-disruptive (or positively disruptive), visible, and effective they are. Try to have a few done before you start your 90-day outbrief. You should have an ongoing stream of quick wins until some of your longer-term projects start to bear fruit.

Obvious Projects

Odds are, you were hired for a specific reason, often to fix specific problems that everyone sees. These are going to be the backbone of your security program for the first 12-24 months (if they were really easy, they'd be done already). Make sure you've identified who your partners in execution are, and that they are bought into your plans, and will be there to support you.
It can be tempting to lump everything into this category, but you really don't want to spread your team too thin. Be realistic about what you could get done, and then cut that in half when you're planning. If you are too conservative in your estimates, you can always get more done, but getting less done than you advertise early may be problematic for you.

Long Term Changes

You've probably also identified a number of structural changes you want to make. Be very careful about how you evangelize these projects, especially if they are going to require strategic changes across your business. Figure out if there are Quick Wins or Obvious Projects that let you get started on your changes, without needing to sell the business on big, disruptive programs before they have confidence in your ability to execute.

Restructuring

Governance

If the organization doesn't already have a Cyber Risk Committee, you'll want to establish one. This should be you and your primary stakeholders, likely executives responsible for IT, Engineering, Operations, HR, Trust & Safety, Privacy, Internal Audit, and Legal/Compliance. If you have broad oversight in the business, this might be the C-level executives; it could also be director-level peers in a more tactical role.
The mission of your Cyber Risk Committee is principally to ensure business-wide alignment on cyber risk in your business. Tactically, that means that before you brief new projects upward, the Cyber Risk Committee should already be aware of those projects, and in agreement that those risks make sense.

In some businesses, the Cyber Risk Committee is really two different groups. One is the official committee, which consists of the senior executives, and they meet rarely, perhaps once per quarter, to review and synchronize as part of your Board reporting cycle. You'll brief them on what's happening in the business, changes to the risk profile, and perhaps collect some input as you plan for new major initiatives.
The second group is often made up of senior staff from each of those functions. Your direct reports, and the directors/VPs/architects who are directly responsible for security in each of the functional areas. This group coordinates the work that is actually happening, and responds to investigate new areas of risk or environmental changes.

If the company already has an executive-level Enterprise Risk Committee, you'll want to connect your Cyber Risk Committee as a working committee of the Enterprise Risk Committee, and you'll often have significant overlap in membership. Learn the cadence of the Enterprise Risk Committee, and ensure you set up your Cyber Risk Committee for success.

Your Team

There's a good chance that you're going to need, or want, to change the configuration of your team as part of implementing your plan. You have three fundamental choices in approach.

- You can be transparent, and let your team be part of planning. You might involve just your leadership team, or you might involve the whole team. Take this choice if you have great

people, but they are doing work that isn't as effective as you need. You want to keep them engaged, especially if their work will change, and having them bought into the changes will be critical.

- You can be quickly opaque, and do your planning mostly in secret. You'll then execute fairly quickly, moving on from people who don't fit your idea of where the team is going, and then hiring new people into new roles. You might need to take this path because you were brought in to replace the existing team – maybe their philosophy didn't match where the other executives were – but you should be cautious. Even the people you want to keep will be worried by this approach, and you'll probably suffer even higher attrition than you expected. You aren't going to get as much done in this model as you might expect, especially since you'll need to spend a lot of time hiring.
- You can also move slowly. You can often use a budget increase to create new roles in your organization, and incentivize members of your existing team to take those roles. You can let your people know which functions in the team are going to be lower priority (and won't receive guaranteed backfills), so that overly large groups can more naturally thin out through transfer or voluntary attrition. This approach takes the longest to reach steady state, but is usually the least disruptive. You may still have to actively manage out people who aren't the right fit for your future organization, but you can often do so with more grace.

Socialize Your Plan

No matter how brilliant your plan is in your head, it won't be effective if you don't communicate it well and evangelize it properly. This isn't a one-time activity, where you give a presentation accompanied by a beautiful slide deck, and then you're done. Rather, socializing your plan is a continuous process, one that actually begins *before* you start, and will continue until the day you depart. That said, there are certain points where you'll need to share your plan with some specificity. Your goal should be to have three levels of specificity that you can talk about your plan with. At the high level, you just discuss your framework. At a medium level, you'll discuss your initiatives. At the detailed level, you'll talk about specific projects.

Alongside the plan that you're socializing, it's reasonable to also present your assessment – after all, it's the things you learned that are driving your plan, and you may need to connect the dots for your stakeholders. While measurements can be helpful in telling your assessment story, don't rely on them – if the security program's changes were trivially decidable by metrics alone, there wouldn't have been a need for a CISO.

> *TIP: Make sure you use the official corporate slide templates, even on Day 1. Connect with the designers in the Creative Services team in Marketing if you need help on making beautiful slides. All words on your slides should be, at minimum, 12 or 14 point fonts, easy to read. Do not use slides for walls of text, that's what you have documents for.*

Vision and Mission

You need a clear and simple way to articulate the values of your team, and what you'll be prioritizing. Vision, Mission, and Values statements are clean ways to do this (see chapters 40 & 41 of *1% Leadership* for more in-depth guidance), and you'll definitely want to articulate the Vision and Mission for your stakeholders. You can think of a Vision statement as a definition of *who* your organization will be, and the experience your stakeholders should expect ("InfoSec exists to be a helpful, sustainable guide"), while a Mission statement is define what you'll achieve ("Creating seamless safety that enables growth while minimizing disruption"). In your first 91 days, it's okay if these are more personal: *your* mission and vision, and over time they'll evolve to be your organization's vision and mission.

Framework

Even before you start, you likely already have a framework in mind. You should be able to create a simple slide to show your framework. It should be a clean and simple model that people will easily remember after meeting with you. Perhaps you have three pillars: Stabilize (keep what's working), Modernize (replace ineffective or expensive-to-maintain legacy solutions), and Optimize (streamline process and automate where possible). The framework should be heavily influenced by what you heard your executive stakeholders say during the interview process. If they asked a lot of questions that revealed they wanted to know more about what was happening, perhaps Transparency becomes one of your core pillars.
Not everything in your security program needs to be explicitly called out in your core framework, but you should not have large swathes of your organization wondering where they fit in your priorities.

> TIP: Some people respond very negatively to the word "pillars" in describing a new executive's program. You can make it up and call them "focus areas" or "principals" to keep away from the negative reaction.

The Role of Initiatives

For each pillar in your framework, you'll first need to dive a level deeper. Your Initiatives are collective groupings of projects under a thematic pillar. For most of your stakeholders, this is just to provide a level of abstraction Under a Modernize pillar, for instance, you might have an Initiative for "Update Internal Tools to Current Best Practices" which is going to collect migration projects for the tools your team created – perhaps into a standard code repository, updating outdated software libraries as you go. Teams that use your tools will be very interested in the details, even if this is a low priority; while other stakeholders are likely to barely want to see the initiative at all.

> *TIP: Sell your high priorities with eye-catching Initiative names. "Remove Security Obstacles" is a catch-all for anywhere that you're getting rid of an ineffective process; "Stop Ransomware" might be a compelling initiative to capture a set of projects that everyone will line up behind.*

Into the Weeds

While not every stakeholder will care about every project that you intend to drive, every project should have at least someone who needs to know about it. For each project in your plan, you should, at minimum, document a few things. You should have a simple description (The project "Convert SSO to FIDO2-MFA" may have a description "Upgrade our single sign-on infrastructure so that we use *possession*-oriented authentication, eliminating passwords"), an explanation of why this is important ("Risk: current SMS-Push 2FA system can be attacked via phishing and SMS spamming"), a set of milestones along the way, and, most importantly, the success criteria, documenting in advance how the organization can measure success ("all systems that use SSO support new FIDO2 MFA architecture"), which may have explicit exceptions ("systems that do not use SSO currently are not in scope for this project").

If a project becomes high-profile, you have a simple and easy way to communicate about it now, and a simple description like this becomes a contract between you and your stakeholders.

Buy-In Along the Way

As soon as you write anything into your plan, you should identify who needs to know, and tell them first, ideally by having already discussed it with them. A simple rubric for identifying that list of people from whom you need buy-in is to determine who would be surprised if they heard about a given project from someone that wasn't you. Make sure they see what's coming. Hopefully, this is just a courtesy conversation, because they've asked you for the project, or you collaboratively identified the need for it, but a big part of your goal here is to eliminate any surprise.

Sharing with Stakeholders

Now comes the fun, and scary part: socializing your plan. Unless your plan involves burning down your team, you should always start with your team. You should show them what's still a draft, and what you have commitments for from stakeholders. The first sketch of your plan should be visible to your team within the first month (even while it is mostly tentative).

The draft that you're going to review with your peers should be ready by the end of the second month, where you'll aim to get buy-in and agreement on success criteria. If there is anything on your plan that requires one of your peers to agree to, make sure you've met with them, and gotten their agreement, long before you start showing it to your mutual peers.

On Day 91 – three months into your tenure – you'll have your final plan ready. This one is going around to the executive stakeholders;

but most of them you should have shared it with individually before you do any form of group presentation. You'll want to brief your company's executive team, preferably in front of each other. While they've all agreed in private, making sure they agree in front of each other will be important for you to maintain your progress.

On To Your Next 91 Days

Congratulations on surviving your first 91 days as a CISO. Hopefully, you'll be able to apply the practices that you started your tenure with to the rest of your stay as a CISO; this isn't just a one-and-done process. You should be continuously learning about your environment, getting feedback from your stakeholders, identifying ways to improve, and tracking and measuring your program's efficacy.

In the interest of brevity, I skipped over a lot of really important work you'll need to also pay attention to, so I at least wanted to leave you with a quick summary of what might come in the next volume of the How To CISO guide, assuming you all leave favorable reviews on this volume.

- Metrics, risk quantification, and risk qualification (describing risk without trying to measure it)
- Reporting to the Board
- Personnel Development
- Landing the perfect gig

You can find me on Twitter or LinkedIn as *@csoandy,* and I'd love to hear from you about what you found helpful, and what you wished I'd added.

First 91 Day Checklist

This is a starting point to help you identify what you should get done, and in what rough order. If you have a Chief of Staff, an Office of the CISO, or even an executive assistant or project manager, let them help you keep on track here.

- Week 1
  - All-Hands meeting with your direct organization.
  - Schedule appearing at team meetings within your organization.
  - Schedule meetings with your peers and stakeholders.
  - Create a sketch framework to fill in your plan.
- Week 2
  - Meet with your peers and stakeholders.
- Week 3
  - Meet with your peers and stakeholders.
  - Identify your first proposed Quick Win.
- Week 4
  - Meet with your peers and stakeholders.
  - Socialize and pressure-test your first Quick Win.
  - Schedule Week 13 briefing to senior management stakeholders.
- Week 5
  - Review your findings and draft plan with your team.
  - Commit to your first Quick Win.
- Week 6
  - Define your strategic plan for the next 18 months.
  - Execute on your first Quick Win.
- Week 7
  - Identify what benchmarks you will use to measure your plan.
- Week 8
  - Stakeholder buy-in on Obvious Projects in your plan.
  - Identify second Quick Win. Socialize and pressure-test.
- Week 9
  - Execute on your second Quick Win.
- Week 10
  - Conduct a quick gap analysis on your plan against your assessment of the business. Be prepared to defend your prioritization choices.
- Week 11
  - Socialize plan with individual senior stakeholders and direct reports.
  - Identify and socialize your third Quick Win.
- Week 12
  - Socialize plan with individual senior stakeholders and direct reports.
- Week 13
  - Socialize plan with senior stakeholders.