CYBERSECURITY PROGRAM

An introduction

[DATE]

NAME:

INFO 6027 W2023 Assignment 3

Contents

Cybersecurity Program Development for Business

Understanding Risk

Studying risk is taking a trip down a fascinating, complex, and intricate labyrinth. It is hard-core science—involving complex mathematics, ethics, and philosophy—with potential life-and-death implications (e.g., the risk of reprisals when we attack a terrorist group, the risks that first responders take every day, etc.)

Risk is the combination of the likelihood of an event and its impact.

What's the risk of a hurricane in Miami? Well…how likely is it, and what will its impact be when it hits? Why do you need know this? Because, for starters, the answer determines whether you want to move there, if you want to start a business there, if you want to send your kids to school there, and how much your insurance will cost you to protect you from this risk, and so on.

How can you determine the likelihood that a hurricane will strike Miami? You have statistical data that give you a good sense of the frequency of hurricanes hitting the area over the past couple of hundred years.

What's the impact? There is the cost of rebuilding, the cost of business losses, environmental damage, and the potential of loss of life, among many others.

To summarize risk definitions:

- *Asset*: Anything of value
- *Risk*: Likelihood of an event, multiplied by its impact
- *Mitigated risk*: Existing risk after controls have been applied
- *Residual risk*: What's left over after risks have been mitigated or transferred as much as possible
- *Accepted risk*: Residual risk that has been accepted, aka *the risk of doing business*
- *Controls*: Active countermeasures, be it processes, systems, or applications, that prevent, detect, correct, or compensate against risk

What is it worth to the business?

Dreadful statistics showing how cybercrime is increasing by the day.   Ransomware attacks are one of the fastest-growing cyber threats in recent history — **reports of ransomware incidents increased 62% in 2021 compared to 2020**. Ransomware was also the third most used cyberattack method in 2021, accounting for 10% of all data breaches.

Today, the concept of *value* has expanded beyond tangibles to include intangibles such as data, intellectual property, and reputation. As a matter of fact, many intangibles hold more value than tangibles.

What is a Digital Ecosystem? *Hardware, Software, Network, Digital Services, Hosting and Cloud, 3rd party vendor (connects into your network).*

- *Hardware*: Any physical device that can store, process, or transmit data in digital form. Examples include everything from supercomputers to personal computers, laptops, tablets, cellphones, wearables, switches, routers, and digital appliances of every imaginable (and some unimaginable!) kind. Going forward, and as a matter of convenience, I will be using the term *digital device* as synonymous with *hardware*.
- *Software*: In its broadest definition, software is a set of instructions that guide hardware in performing a task. Nothing happens without software. Think car and driver. You may be familiar with the distinction between the operating system (OS) of a computer or phone and its applications (or apps), but while they are indeed different, both are software; they just do different things. The OS is the software that controls the use of the actual hardware while the applications make requests of the operating system to have the hardware perform specific tasks.
- *Network*: In this context, a network is a collection of connected (again, most often digital) devices. You can have a network of computers—such as the one in your office that enables you to send a document to your office printer—and you can also have a network of networks—such as your point-of-sale terminal network that connects to a credit-card authorization network. Whatever its size, the point of a network is to enable communications. Networked devices can share data and software, leveraging their connection to increase processing power. The Internet is a network of networks. In fact, it is *the* network of networks—you might think of the Internet as one giant ocean but in fact it's more like a huge number of interconnected streams, rivers, and lakes. And like Tolkien's “one ring,” the Internet is there connecting them all!
- *Digital Services*: Simply put, a *service* delivers value to a customer through action (a human doing a task for the customer) as opposed to manufacturing (producing a product). Similarly, for digital services: A collection of hardware and software, networked or not, combines to deliver value. For example, a digital service can be something as simple as digital storage. Other digital services include access to processing power or to a particular application.
- *Hosting*: Be it a business (such as hosting a website) or a service (hosting storage), the term *hosting* means the capacity to deliver digital services located off-premises (remote) to the consumer. There are many nuances to the term (for example, *near hosting, far hosting, distributed hosting*), but the easiest way to think of it is that the computers are located in someone else's office—that office hosts the computers on your and others' behalf. That other firm runs and maintains them, pays the electric bills, and so on—while you get to use the computers by accessing them remotely.

- *Cloud*: Or, cloud computing, is the delivery of hosted digital services, on demand, over a network, and commonly over the Internet. If these services are being delivered through private and proprietary means, then the term used is *private cloud*. If the network is the Internet, then it's called *public cloud*. If we combine them, we refer to it as a *hybrid cloud*. Terms like Software as a Service (SaaS) and Infrastructure as a Service (IaaS) are now used to differentiate between cloud-delivered application services and hardware services.

The “as a service” tag is getting appended to more and more digital services these days, for example, Architecture as a Service (AaaS), Platform as a Service (PaaS), and Everything as a Service (XaaS). The main advantage of cloud computing is its scalability, redundancy, reliability, pricing, and on-demand availability. The main disadvantages are that all of these “as a services” are nothing more than “hosted subscriptions,” rather than items you own. “As a service” is kind of like renting an apartment in a location you can't always control, with co-tenancy issues (you moved from your apartment to one with roommates), conflicts of interest (the renter has different priorities from the landlord), and potential problems with accessibility (no Internet access means no cloud access).

Cybersecurity can be defined as…

Cybersecurity is the ongoing application of best practices intended to ensure and preserve confidentiality, integrity, and availability of digital information and the safety of people and environments. The four best-practice pillars: *confidentiality, integrity, availability,* and *safety*.

Security is a practice dealing with all aspects of prevention, protection, and remediation from any type of harm to an asset. The bulletproof glass in front of the Mona Lisa is security.

Information security is also a practice, one that aims to protect any type of information assets. The fireproof safe where you keep your will is a form of information security.

Cybersecurity is a subset of information security, focusing specifically on protecting digital information assets in their ecosystem.

How to measure Cybersecurity success?

The easiest example of a goal is sales. It's a number. You either hit it or not. If not, you can measure how far away you are from making that number. So, if your goal as a business is $10,000,000 revenue, and your key goal indicator is currently at $5,000,000, you're 50 percent there! (Hopefully, you also have six more months to go before having some explaining to do.)

Now, what are your CSFs for this goal? There can be several. One may be, “We need two new clients per month.” Another may be, “We need to increase existing client spend by 10 percent per month.” And, another may be, “We need to reduce cost by 20 percent through automated service delivery.” All three could be CSFs. Which one do you focus on most? Are they all equally weighted? CSFs will influence how resources are directed toward goal achievement, so you need to be particularly careful in making sure that they are clear and widely disseminated. Otherwise…you guessed it! Out of alignment.

Finally, your KPI tells you how well you're tracking against those critical success factors. If the CSF is “Increase existing client spend by 10 percent per month,” then you can run a monthly KPI report that tells you if this has been met. Same with any (well-selected) CSF.

In summary:

- *KGI = key goal indicator***=** Metric of progress toward achieving your goal.
- *CSF = critical success factor***=** Metric of impact toward achieving your goal.
- *KPI = key performance indicator***=** Metric of course deviation from achieving your goal.

Now, you may ask, do I really have to do all this? Do I need all these measurements and acronyms and tracking, and this, that, and the other? Yes! You do. But, don't worry. You're doing this already. This is simply putting it in more formal language. Even if you are a small, informal business, you have goals, KGIs, CSFs, and KPIs. You may not call them that, but you do. Your financial statements prove it! So does your success, your challenges, and even your failures. You use these tools—no matter what the terminology—to navigate your own world every day.

Why be all formal and keep track of all this? Because, at the end of the day, you cannot improve anything that you cannot measure.

Why should we consider a framework?

Think of frameworks as playbooks. Take football, for example. You have the rules of the game, and each team has a playbook. Consider that playbook the specific team's framework for winning. Not all playbooks work well for all teams, yet all teams must obey the same rules of the game. This is an important distinction, and it applies equally well in business.

A good framework should be comprehensive, flexible, adaptable, and straightforward to implement. Although not a complete list by any means, some of the better-known frameworks are: COSO (Committee of Sponsoring Organizations of the Treadway Commission), ITIL (Information Technology Infrastructure Library), BiSL (Business Information Service Management Library), CMMI (Capability Maturity Model Integration), COBIT (Control Objectives for Information and Related Technology), TOGAF (The Open Group Architecture Framework), and PMBOK (Project Management Body of Knowledge), which is more focused to the project management discipline but still overlaps with IT management and good management practices in general.

Defense in Depth.

The best way to use all these controls is by layering them across systems in a way that achieves what is called defense in depth. This has the effect of putting multiple and diverse barriers (controls) between the attacker and the asset.

What are controls and why we need them as part of a cybersecurity strategy?

First you develop a strategy that's right for you. What does this look like? It depends on your business. As you would expect, cybersecurity strategy will vary greatly from business to business, just as marketing strategies or daily operations vary from firm to firm. No two companies are exactly alike, even within the same industry. What is right for one law firm may be too much for another. One may be dealing with intellectual property (IP), trademarks, and patent law, versus another that may focus on criminal law, and a third on tax and estate law. All want to be secure, of course, but the priorities and data life cycles can be very different.

You'll recall that controls are actions that mitigate risk. They will prevent, detect, correct, or compensate against risk. More specifically:

- *Preventive controls* are designed to prevent the attack from reaching the asset in the first place. A nondigital preventive control might be a pair of big burly guys, armed to the teeth, who physically guard your assets. Digital preventive controls include, as we already discussed, cybersecurity awareness training as well as more technical controls like firewalls, intrusion prevention systems (IPS; designed to both detect and thwart an attack).
- *Detective controls* are designed to identify that an attack is occurring, including what kind of an attack, where it came from, what it used, and, if you're lucky, who may be behind it. For example, motion detectors that set off sirens waking up the aforementioned big burly guys and send them to go chase the intruder are detective controls. These days, these motion detectors can take the form of sophisticated cameras, detecting motion, plus capturing images and sounds. Digital detective controls include antivirus and antimalware systems, as well as intrusion detection systems (IDS; designed to detect abnormal patterns in networks or systems and raise the alarm).
- *Corrective controls* are designed to minimize the damage from an attack. Examples include restoring from backup, patching the systems with the latest security fixes, upgrading to the latest version of applications and operating systems, and the like.
- *Compensating controls* are designed to compensate for the failure or absence of other controls and mitigate the damage from an attack. Examples include having a hot failover site (a geographically separate site that mirrors your environment, available the instant

you need it), isolating critical systems from the Internet (aka air-gapping), and, in general, backup and disaster recovery plans that can keep the lights on while everyone else is in the dark.

Threat Agents

Who is out there? What harm are they attempting to cause you and why? As you would expect, threats vary business to business: The threat context for a restaurant is going to be quite different from that of a brokerage firm or a utility company.

It's important to distinguish between a threat (the impending prospect of something bad happening) and an attack (the realization of a threat). Keep in mind that cyberattacks are not accidental—they don't just happen; they are planned. Cyberattacks involve organized efforts by someone(s) to accomplish something particularly wicked regarding your digital assets. Attackers will be stealthy, they will be persistent, and they will not stop unless they are either successful or busted.

The people behind such cyberattacks are called a lot of things, but this is a family book, so we'll stick to threat agents.

Current trends influencing Threat Agents

1. **Cybercriminals**

   Motives: “Show me the money,” plain and simple.

2. **Insiders (e.g., employees)**

   Motives: money and revenge, not necessarily in that order.

3. **Nation-States**

   Motives: cyberwarfare or intellectual property theft, competitive intelligence gathering, etc.

4. **Corporations**

   Motives: cyber-corporate-warfare or intellectual property theft, competitive intelligence gathering, etc.

5. **Hacktivists**

Motives: activism of one sort or another, often but not always altruistically motivated (freedom of speech, fight against injustice, etc.).

6. **Cyber-Fighters**

   Motives: nationally motivated “patriots” like the Yemen and Iranian Cyber Army.

7. **Cyberterrorists**

   Motives: to create fear, chaos. Terrorist by any other name.

8. **Script Kiddies**

   Motives: young people “hacking for the fun of it” and causing havoc, be it intentional or not.

The nature of present-day hackers?

Back when the Internet was a cyber–Wild West, the term *hacker* was no insult—quite the opposite, it was a term of respect. The Internet as we know it was created by people who proudly called themselves hackers because a *hacker* was anyone skilled at building, exploring, and expanding the capabilities of all sorts of systems.

Nefarious, bad-guy hackers should really be referred to as thieves, vandals, criminals, really-really-really-bad people, etc. Unfortunately, the distinction between good hackers and bad hackers never caught on, and these days the term *hacker* is usually not meant as a compliment. But not all hackers are alike: The differences between them can be night and day, black and white, Jedi-versus-Sith, or your choice of fundamental opposing forces.

Historically speaking, all hackers *do* have one thing in common: high levels of technical skill. Hackers explore the details of programmable systems and figure out how to stretch their capabilities. This is very important because the skills involved are far from inconsequential. It requires a combination of inborn talent and endless study, competition, and practice. All great hackers, irrespective of which side they are on—night or day, good or evil, black hat or white—share these hard-won attributes. You might not be surprised to learn then that many old-school hackers have been recruited (or volunteered) to solve some of the world's most intractable problems such as curing diseases, distributing vaccines, or developing next-generation safe nuclear reactors.

Hackers also, it should be said, tend to have very healthy egos and are usually not above showing off their skills. Knowing a bit about the hacker personality helps set the context for your cybersecurity program and—importantly—how you communicate about it.

Attack examples

- *Advanced persistent threat (APT):* An APT says what it does and does what it says—it's a coordinated, persistent, resilient, adaptive attack against a target. APTs are primarily used to steal data. They can take a long time to research, plan, coordinate, and execute, but when they succeed, they are frequently devastating. You definitely do not want to be on the receiving end of one, and if you are, you had best have a very strong incident response plan in place.
- *Brute force attack:* If there is any elegance in hacking a system, then this method lacks it. A brute force attack, much like a brute, doesn't use any brains, only force—in this case, computing force. So, if I wanted to guess your password with a brute force attack, I would use a very fast computer to try every single combination possible of the number—a task that can take a large amount of time or a startlingly brief amount, depending on the complexity of the password. For example, a 4-digit numerical PIN takes only a few hours to crack by brute force. (If you would like to test your own password or PIN to determine how long it would take for a brute force attack to crack it go to http://passfault.com, an open web application security project (OWASP) site, and give it a try.)
- *Denial of Service (DoS) attack:* DoS attacks come in two flavors: single-source and distributed. A single-source DoS attack occurs when one computer is used to drown another computer with so many requests that the targeted one can't function while a distributed DoS (DDoS) attack achieves the same result through many (meaning thousands or millions of) computers. In DDoS attacks, the computers are usually under the coordinated control of a botnet (see “A Brief Cyberglossary of Terms” in the next section), working together to overwhelm a target with requests, rendering the target computer inoperable. Of late, this type of attack has gotten more and more press because instead of using compromised computers as part of the botnet, the hackers have been using any digital device (such as nanny cameras, thermostats, etc.) that is connected to the Internet. Most of these devices lack even the most rudimentary security, and too many users don't bother changing the default password, further contributing to the ease of compromising these devices and using them as bots.
- *Man-in-the-Middle attack:* In this type of an attack, the hacker intercepts the communication between two systems, replacing it with his own, eventually leading to his gaining control of both systems. For example, a man-in-the-middle attack can be used to gain access to credentials and to then fake normal operations while the attacker compromises the target.
- *Phishing attack:* Phishing and spear phishing are attacks that use social engineering methods. *Social engineering* in this context is just a fancy word for lying. Hackers convince a victim that the attacker is a trusted entity (such as a friend, established business, institution, or government agency) and trick the victim into giving up their data willingly. The goal of these attacks is to gain your trust so that you divulge sensitive information to the attacker. The degree of sophistication of such attacks varies, from

the infamous appeals for bank information from Nigerian princes, to emails that appear to be from a bank or the Internal Revenue Service, to extremely sophisticated cons that can trick even the best-prepared and skeptical victim.

Governance, and why it matters in a cybersecurity program

Governance is the collective set of principle-guided actions that when applied guide a company to the fulfillment of its goals. I use principle-guided actions to distinguish governance from reactive management. I use “applied” to further drive home the idea that governance is something you need to think about, agree on, and consistently apply to get the results you want. These principle-guided actions include a company's strategy, ways to measure success, ways to manage risk, and ways to exercise due care of company assets.

The difference between management and governance is in the “apply” part. The application of governance is what I call management. It is very important to separate the two: Governance is the collective set of principle-guided actions while management is the application of these principle-guided actions into the company's operations.

Although governance is frequently thought as overarching (i.e., across the whole firm), governance filters down and applies to each and every department as well. You need good governance in your IT department, in your cybersecurity department, in your marketing, product development, finance, facilities, etc. Management feedback, of course, is critical in both validating and influencing future governance, and it is this feedback loop that is absolutely essential in ensuring alignment.

Now, please remember: Bad governance will not invariably result in bad management. You can have a poor set of principle-guided actions that are very well applied. Similarly, good governance does not automatically result in good management. They are different things, both equally important. Why? Because if either of them is not up to task, then alignment suffers.

I keep referring to this alignment. What exactly is alignment, and why is it so important? I view alignment as the quintessential metric of value creation. A misaligned company is, at best, inefficient at value creation, and at worst…out of business!

Consider, for example, a company with a clear vision and mission statements, well funded, good, hard-working people, and with an excellent IT manager. She has gone out and procured state-of-the-art systems from top-tier vendors with the corresponding support agreements. She has bought the best her budget could get. Yet, all departments are complaining that nothing can get done in time. They find the systems onerous, and incapable of doing what they—the users—need. Where did the IT manager go wrong?

She didn't! She's managing the department just fine. Unfortunately, in the absence of proper governance, which would have ensured an alignment between IT and business goals, she was left to guess as to which system would be the best fit for what she thought the business needed, and with what she knew technology could provide.

Both governance and management are shared responsibilities. Governance must clearly spell out the set of principle-guided actions that need to take place for value to be created. Only then can management effectively integrate these into business operations. Similarly, if management fails to understand or properly implement what is being spelled out by governance, and give prompt and accurate feedback, then we'll have operational failure. Both cases damage the ability of the company to create value. Both cause misalignment.

Overview of a basic Cybersecurity Program (provide some commentary for the following):

- **Vision and Mission Statement**

A mission statement is your company's *raison d'être*. It's as existential as it gets. It tells the world why you exist. A vision statement, on the other hand, is more directional than it is existential. One is *who and why we are,* the other is *what we are*. The website TopNonProfits.com has collected the top vision and mission statements for several nonprofits. I have taken a few and paired them up to show the difference between mission (top) and vision (bottom) statements:

ASPCA

- *Mission*: To provide effective means for the prevention of cruelty to animals throughout the United States.
- *Vision*: That the United States is a humane community in which all animals are treated with respect and kindness.

Cleveland Clinic

- *Mission*: To provide better care of the sick, investigation into their problems, and further education of those who serve.
- *Vision*: Striving to be the world's leader in patient experience, clinical outcomes, research, and education.

Creative Commons

- *Mission*: Creative Commons develops, supports, and stewards legal and technical infrastructure that maximizes digital creativity, sharing, and innovation.

- *Vision*: Our vision is nothing less than realizing the full potential of the Internet—universal access to research and education, full participation in culture—to drive a new era of development, growth, and productivity.

Feeding America

- *Mission*: To feed America's hungry through a nation-wide network of member food banks and engage our country in the fight to end hunger.
- *Vision*: A hunger-free America.

Smithsonian

- *Mission*: The increase and diffusion of knowledge.
- *Vision*: Shaping the future by preserving our heritage, discovering new knowledge, and sharing our resources with the world.

Now, there are those who will argue that mission and vision statements are a waste of time. There is one goal, and one goal only: Make money. The end. After all, as one executive director of a national nonprofit told me, *"No money? No mission."* I agree. There is truth to the "make money" imperative. But is it your—or your company's—true mission? Does it reflect your company's vision? (If so, write it down.)

From our perspective, this is the starting point of establishing what's of value to you. This will be vital later, when we establish the right level of protection for it.

- ## What is at Risk?
- This is the part where you get to walk around and pose this question: "How much is *this* worth to you?" *This* is the asset you're interested in protecting, and the only one who can determine its worth is the person who owns it.
- Without getting overly complex here—after all, this is only the overview chapter!—the asset owner is the person who, one way or another, is responsible for the asset. For example, the CFO is responsible for the financial assets of the company. What are those? They can range from simple things like Excel spreadsheets, access to the bank accounts, and the accounting system files all the way to massive ERP (enterprise resource management) applications. The CFO is the one who is responsible for all of this, and she's the one who can tell you how much these assets are worth to her. By *worth* I don't really mean monetary value. I mean things like: How long can she be without those assets, how much data can she afford to lose, and, in cases of loss, how quickly does she need to be back in business?
- Where do you start this risk assessment? First, identify your business managers. Each one will typically be responsible for a line of business or a department. Sit down with each one and ask him or her to identify all the things that are absolutely necessary to do their jobs. The list is likely to include multiple assets, both hard (computers, facilities,

etc.) and soft (software, workflows, etc.). You should work with each manager in ranking and prioritizing each asset. At the end of these meetings, you will have a very clear idea of each department's assets, and the corresponding impact of each asset's loss.

- If you want to get formal about this, you can ask for a department-by-department business-impact analysis, and from the results, you can derive both the assets and the business impact of their loss or disruption. But what fun is that? Make it personal and get in there! Roll up your sleeves and work with your colleagues in getting all this done. You'll certainly gain a better understanding of what's going on with the business, and make a whole bunch of new friends. (Or, enemies, if they don't want to be bothered…but hey! You're the one trying to cover their assets! They'll see the light eventually.)
- Okay, you're almost done. You've made tremendous progress in gaining an understanding of your organization, more than most employees or even managers ever do. You should celebrate. Go have a nice lunch. Nothing crazy, though: There is still work to be done. Skip the martinis.

- **Asset Valuations**
- A good first step will be to get a grip on the total universe of our cyberassets. What is included in our definition? Cyberassets would typically fall into one of the following categories: data, hardware, software, systems, processes, and workflows.
- **Data**
- It is important to differentiate between *information* and *data*. Frequently, people use the terms interchangeably, and that's okay for everyday use, but we should be clear on the distinction because the implications can be significant.
- Data, in one sense, is information that has been captured, stored, and represented in some medium. Data is often an expression of information, but that doesn't mean that data is a complete representation of that piece of information. Consider a pot of boiling water. I have a sensor in the pot that measures the temperature of the water and transmits this datum, which is stored in my system in a field called “water temperature.” That's data! But there's a lot beyond the number that we could notice about the actual physical event of boiling water: the magic of phase transition from liquid to gas; the beauty of the rising bubbles; the mathematics of turbulence of the water's surface, and so on. That's all *information* about the boiling water…but it's not data.

Hardware

Hardware is all the electronic equipment that stores, processes, or transmits data. It's also the stuff that controls other stuff, such as thermostats, and all the fun gizmos that make the Internet of Things possible. Why did I limit myself to “electronic” just now? Okay, you got me! Computer hardware can also be mechanical or even quantum. But unless you're Charles Babbage building the Difference Engine or you work at an advanced computing facility, electronic hardware is the only kind you need to worry about.

Software

Software is the applications—from operating systems to apps—that use hardware to get things done. This includes, of course, software that runs in the IoT.

Systems

A system is a collection of hardware, software, and networks that processes data. Systems can be internal or external, and they are frequently a combination of both.

Processes and Workflows

Those are the sequence of steps involved in the creation, transformation, processing, storing, and transmitting of data across systems. The definitions for process and workflows can be confusing, but as far as we are concerned, processes and workflows are assets that contribute value to the company, and as such, are worthy of careful consideration and protection.

How exactly do you protect processes and workflows? It depends! The first step, no matter what, is knowing about them, that is, documenting and cataloging them. This step will reveal any dependencies on systems that these processes and workflows may have. Your thinking about protection starts there, and it cuts both ways: How does the process affect the system and how does the system affect the process? We'll look at this closer when we discuss controls. For now, keep this in the back of your mind and think about concepts like business continuity and disaster recovery.

Asset Metadata

Now that we've listed our universe of assets, what do we need to know about them? When I do an asset classification and valuation, I insist on knowing at least the following 10 pieces of information. I call these the *asset metadata:*

- *Owner:* Who is the owner of the asset? If we're talking about a root-level digital asset, like a finalized product (e.g., a product design, a filing for litigation, financial statements, etc.), then the owner is the enterprise. If, on the other hand, we're discussing a value-generating system such as an e-commerce website, a medical records system, or a content management system, then the owner may be a business unit. More on this when we discuss business-impact analysis further on.
- *Custodian:* Who is the custodian of the asset? The custodian cannot be “the enterprise” in general. It's always an identifiable person, department, business unit, or vendor. You need to be able to say, “Fatima is the custodian—go get her!”
- *Location:* Where is the asset geographically located? This is key, especially if the asset ends up living in the cloud. Again, be specific.
- *Confidentiality Classification:* Rate the asset 1 through 4: public, confidential, secret, or top secret.

- *Criticality Classification:* Rate the asset 1 through 4: nice-to-have, optional, essential, or mission critical.
- *Impact Classification:* This is a pain measurement on the asset's unavailability, corruption, or destruction. A rating of 1 through 4 works here, too: If the asset were suddenly unavailable or damaged, would the pain be none, minor, moderate, or severe?
- *Maximum Tolerable Downtime (MTD):* This is the point in time at which if the asset is not recovered, the impact becomes severe.
- *Recovery Point Objective (RPO):* This is the particular point in time you'll need the asset to recover to.
- *Recovery Time Objective (RTO):* How long you are willing to wait before getting the asset back into production?
- *Resources:* Who will be needed to bring the asset back to life within the RTO and at RPO? Remember, be specific. Use names!

I am going to let you in on a little secret. Those are exactly the same 10 questions that I want to know when I am doing a business-impact analysis, business unit by business unit.

The difference? When I am doing an asset classification and valuation, I am looking at root assets—assets of value at the enterprise level. When I am doing a business-impact analysis, I am looking more at systems—specifically, systems that are critical for each business unit to contribute to the production of the root assets. Some might argue that the distinction is artificial, and they would be right. But I like to think of the whole exercise as a continuum. Asset classification and valuation feeds into business-impact analysis, which feeds into business continuity and disaster recovery, all of which contribute to a solid cybersecurity program.

After you have collected all of the data for the assets, you are ready to take the next step. Like peeling an onion, you need to perform the same exercise on a business unit by business unit level. This in turn may lead you down even more levels as you discover system and workflow dependencies.

Notice that I have avoided mentioning any specific asset valuation at this point. So far what we have is a spreadsheet of valuable assets whose owner is the enterprise, and a few whose owner is a business unit. We haven't assigned any dollar value; we have only accomplished a listing of important stuff that we'd be loath to lose. Before we start talking dollars and cents, we have to perform the business-impact analysis work.

• Business Impact Analysis

At this point, we move away from looking at enterprise-wide root assets to looking at business units. You could apply the same exact methodology with each business unit, and you would be right. You'd also be tired. Very tired. That's because if you attack a business-impact analysis (BIA) from the start by creating that unit's asset listings, you'll be spending endless hours cataloging and cross-referencing assets into systems, and so on.

I recommend going at it from the top, and digging down only to the point that is useful to your specific cybersecurity program. To do this, you'll need to look at the world from the point of view of systems, not assets. Systems, in this context, encompass all assets: A system, in this case, is defined as the collection of hardware, software, processes, workflows, and people that act to create, preserve, modify, disseminate, and curate data throughout its life cycle.

Say that three times fast, and notice: We added *people*. That's important in a business-impact analysis because when it comes to resources you will need to consider the people necessary for recovery and operations. Now, let's take this definition, and business unit by business unit, identify our top 10 properties, expanded in more detail further on:

- *The owner:* We are now moving past the enterprise as the owner. We're looking at humans! We need to find the one true subject-matter expert when it comes to a specific business unit, system, and assets. No one will know it better than the owner. He or she will know what it takes to run it, where the possible vulnerabilities are, what the impact of its loss may be to them, and by extension, to the company. This is why the owner must lead this identification and classification effort for the particular business unit, systems, and assets. They are also very invested in the longevity and health of their world, which makes them even more in tune with the threats against it.
- *The custodian:* Just as the owner is critical in helping you understand all the nuances about the business unit and its systems, the custodian is critical to providing an ecosystem context. Think of a horse and a barn manager. The barn manager doesn't get to decide who rides the horse (that's the owner's job), but the barn manager is responsible for providing a safe environment, food, water, coordination with the vet, and so on. The custodian is important to you because he or she can provide information that's critical to understanding what it takes to keep the owner's business viable, which in turn will define all sorts of priorities and criticalities (e.g., No hay? No horse! Or at least a very hungry, cranky horse! Don't ride that horse.)
- *Location:* The location of a business might sound like a painfully obvious detail, but keep in mind that location is not just a real estate question anymore. Of course, you need to know the physical location of the business unit, especially if there are multiple locations all over the planet. This information will also provide valuable context (“What do you mean you can't find the CFO in India?”) and exposes all sorts of vulnerabilities that are specific to geography, time, and local regulations.

But beyond real estate, our particular interest is locations in the cloud. Forget the obvious (where *is* the cloud, exactly?), and start thinking about new and exciting terms like *co-tenancy* (your stuff has roommates that you didn't know or approve), *transborder data flow* (your stuff lives on servers in multiple countries), *regulatory* and *compliance* issues (e.g., data in Europe is regulated differently from data in the United States), right-to-audit issues (the cloud provider must agree to your ability to audit), certifications, and so on.

Do remember, please, that if your stuff is in the cloud, then by definition, you are a tenant. This matters because the landlord may have different priorities than you do. For example, imagine that there is a robbery in the building, but not in your apartment; the landlord may or *may not* notify you. Now translate that into digital terms: If your cloud is breached but your specific data is not affected, will you even find out the breach occurred? Wouldn't you want to know?

Bottom line: If your stuff is in the cloud, you will need to do additional homework to make sure you're protected.

1. *Confidentiality Classification:* Like before, I recommend that you use a scale from 1 to 4, with 1 assigned for “public,” 2 being “confidential,” 3 for “secret,” and 4 for “top secret.”

   Two tips: First, avoid the trap of having more classifications than necessary. Keep it as simple as you can.

   Second, use an even number of classifications to avoid giving anyone the option to pick the middle number as a safe bet. Since you're doing all of this work in partnership with the asset's owner, insist that both of you think this classification through and through. You'll be surprised at the dividends down the line.

   If in doubt, use scenarios. Ask what-if–type questions. What would happen if this data was leaked to the public? What is the impact of a payroll report mistakenly being circulated company-wide? Can you identify groups of users with clear delineations for information access? Who needs to know this data, and who should not know? Are there policies in place that delineate access rights to the data?

2. *Criticality:* Again, I recommend that you use a scale from 1 to 4, with 1 assigned for “nice-to-have,” 2 being “optional,” 3 for “essential,” and 4 for “mission critical.” These are applicable across the spectrum, from business units to assets, and you need to be as objective as possible when assigning them. Not all assets are critical. They may all be *valuable,* but that doesn't make them critical. You may be able to operate okay for months without the music server streaming, but be forced to close your doors if accounting can't pay vendors or meet payroll.

   Scenarios are very helpful in establishing criticality, especially when framed by a specific business unit function, that is, limited in scope. If you start talking criticality at the enterprise level, that is, which business unit is more critical than another, then you had best do so only in the presence of the executive committee and the board—otherwise all these friends you worked so hard for are going to be looking at you sideways (e.g., “What do you mean ‘facilities management’ is not as critical as ‘finance?’ Let me see you work with no heat!”).

3. *Impact:* This is the measurement of pain on a scale from 1 to 4, from “none,” to “minor,” to “moderate,” to “severe.” How painful is the outage going to be in terms of business impact? Are you out of business? If so, the impact is severe! Are the fees associated with the outage so high that the business will lose money for the year? I'd call that “severe,” too. The quarter? Let's go with “moderate.” You wouldn't even notice the charge in the P&L? I'd call that “minor.” You should feel free to come up with your own terms, but my advice is keeping it down to no more than four, and to avoid colorful language. Other people, potentially of sour disposition, may read the document someday, and you don't want them raising any eyebrows as they contemplate litigation, especially if the outage will cause a public relations nightmare for your company.

An interesting side note: The business unit owner will assign their version of impact. Then, the executive team may assign a different version of impact for the unit. And finally, the board, which is the ultimate decision-maker on all matters of risk, may choose to accept an impact classification of severe as not worthy of a set of controls, despite your advice to the contrary. Crazy, I know, but these differing points of view are entirely appropriate.

The business unit owner will justly consider a system's failure impact as severe for their unit while the CEO may consider the business unit's inability to contribute value as moderate, and the board may very well accept that risk and elect not to apply any controls toward that moderate or severe impact assessment. There are times when yours is not to reason why.

4. *Maximum Tolerable Downtime (MTD):* Let's assume the business unit is out of commission for some reason—cyberattack, power outage, whatever. Ask the question: "How long can the business unit owner tolerate the outage?" That's the amount of pain that the business owner is willing to accept before things turn ugly. What's ugly? Ugly is going out of business. That's pretty ugly. Less ugly is finding yourself unable to comply with a contract or regulation while more ugly is loss of life because of the outage. You get the idea. The MTD provides a baseline for building disaster recovery and business continuity plans.
5. *Recovery Point Objective (RPO):* The RPO tells you the *when* in time you need to be able to recover to. Think of it this way: Let's say you have an accounting system. The thing goes south on you. It's out. Gone. Nothing is running. Can't pay invoices, can't process receivables, and can't run payroll. The natives are starting to get restless. The IT department and the accounting vendor look at the situation and they tell you that the system will be back in two days' time, and the data will be restored from last week's backup.

   Here's the question you should be able answer to *before* the failure: Is that okay? If so, it means that once you get the system back (in two days) you'll have to reenter all transactions that happened between the last good backup and the day you have the system back. If you agree, that means that you have implicitly accepted two values: One is the recovery point objective of one week.

   The second is:

6. *Recovery Time Objective (RTO):* Your RTO is the maximum amount of time that you're willing to wait to be back in business, or—to put it in a more positive light—RTO is, ideally, how fast you'd like to have the problem go away and you back in business. In the preceding example, you accepted an RTO of two days. This is different from the MTD, which you may have set as one month, because with no payroll for a month, you'll be left with no employees and no business. Hence: maximum tolerable downtime.

   Now, consider that instead of an accounting system going down, you're a brokerage firm, and your brokerage system crashes. No more trades. No more reconciliation. No more portfolio management. You have no idea where the orders that were in the pipeline are, what's executed and what hasn't, what the values are, etc.

What's your recovery time objective? If you said a few seconds, you would be right! Anything more could put you out of business. And your recovery point objective? Right up to the last second before the outage. You can't afford to lose any transactions. (To say nothing about those “men in black” from the regulators who will want to have a friendly chat with you about the outage.)

7. *Resources:* This is one of the most important pieces of information you'll collect. What are the resources (always per business unit per system) necessary for recovery? They need to be accurately identified and be cataloged in an actionable, meaningful way. You'll need not only the “Who is doing what?” question answered, but also how to get in touch with these resources, including backup plans if the resources are not available.

   For example, if your can't-live-without-it custom application was written in Etruscan by Molly, who has since retired to Oahu, it is probably a good idea to: (a) have all of Molly's up-to-date contact information, (b) have identified the last few remaining Etruscan speakers, and (c) reflect on the lesson-learned about keeping mission-critical systems up-to-date and not in dead-and-gone language.

   Similarly, you need to keep in mind that resources will be placed in contention if more than one system goes south (a likely event in the case of a cyberattack).

Now, the good news: You will be pleasantly surprised at how easy it is to collect these 10 pieces of information from a business unit owner. But you will be unpleasantly surprised at the difficulty of collecting same if you have not found the right business owner! In other words, don't necessarily look at the organizational chart and expect that a department head is the right owner of a business unit. That person may be the administrative head, but the *real* owner is someone who not only *takes action,* but has the experience and expertise in the running of the unit.

This is not as unusual as it may sound, nor is it necessarily a problem. There may well be cases, for example, that the vice president of finance is an excellent strategist and an invaluable member of the management team, but it is the controller who is the business unit owner because she knows everything there is to know about it. You need to engage the vice president, be deferential to her, and include her in the process, but roll up your sleeves with the controller by your side.

There are also software applications that you can use to help you with BIA, asset classification, and so on. One important safety tip: Bring your wallet! They tend to be expensive, and frequently part of a bigger business continuity management solution. Don't get me wrong; some of them are excellent, and if the size of your company warrants an enterprise-grade solution, you should look at them. But as far as mid-sized and small-business markets are concerned, at the time of this writing, my recommendation is to stick with my one-spreadsheet-to-rule-them-all solution, which comes next.

One Spreadsheet to Rule Them All

Start by creating one spreadsheet per business unit. The name of the spreadsheet file itself is the name of the unit. All spreadsheets live in the same directory to make linking easy. Your spreadsheet should look something like Table 6.1.

Table 6.1 Example of Business-Impact Analysis Table

Asset/System	**Owner**	**Custodian**	**Location**	**Classification:**	**Criticality**	**Impact**	**MTD**	**RPO**	**RTO**	**Resources**

Each row is taken up by a system owned by the business unit. Owner, Custodian, Location, and Resources can be initials or spelled out. Classification, Criticality, and Impact are numbers 1 through 4. MTD, RPO, RTO are numbers in hours (or minutes, or seconds, depending on the situation; just make sure you're consistent across all spreadsheets).

Additionally, I recommend that you make System, Owner, Custodian, Location, and Resources links to other spreadsheets that contain more granular data, all the way to a single asset. Where do you stop? Wherever it is appropriate for your firm! Remember, no two companies are alike. For example, for one mid-sized company, you may have something that looks like Tables 6.2 through 6.7.

Table 6.2 Example of Business-Impact Analysis Table for Finance

Spreadsheet name: FINANCE										
Asset/System	**Owner**	**Custodian**	**Location**	**Classification:**	**Criticality**	**Impact**	**MTD**	**RPO**	**RTO**	**Resources**
The Books	CM	AM	NY	3	3	3	40	24	48	IT
Payroll	CM	AM	NY	4	4	4	40	24	48	IT
Time Track	CM	SL	CA	3	4	4	20	8	16	IT

Table 6.3 Example of Business-Impact Analysis Table for an Accounting Application

Spreadsheet name: The Books										
Asset/System	**Owner**	**Custodian**	**Location**	**Classification:**	**Criticality**	**Impact**	**MTD**	**RPO**	**RTO**	**Resources**
FIN SERVER	IT	IT	NY	3	3	3	40	24	48	IT

Table 6.4 Example of Business-Impact Analysis Table for a Payroll System

Spreadsheet name: Payroll										
Asset/System	**Owner**	**Custodian**	**Location**	**Classification:**	**Criticality**	**Impact**	**MTD**	**RPO**	**RTO**	**Resources**
PAY SERVICE	IT	IT	MO	4	4	4	40	24	48	IT

Table 6.5 Example of Business-Impact Analysis Table for a Time Tracking Application

Spreadsheet name: Time Track										
Asset/System	**Owner**	**Custodian**	**Location**	**Classification:**	**Criticality**	**Impact**	**MTD**	**RPO**	**RTO**	**Resources**
TM SERVER	IT	IT	CA	3	4	4	20	8	16	IT

Table 6.6 Impact/Criticality Systems Spreadsheet

Impact/Criticality	**Nice to Have**	**Optional**	**Essential**	**Mission-Critical**
No Impact	Lunch ordering	Online 401K review	Building lease and drawings	
Minor Impact	Ad hoc reporting	Expense reports	Travel advance	Inventory control
Moderate Impact	Online ticketing	HR appraisals	HR hiring	Financial systems
Severe Impact	Policies and procedures	Fixed assets	Payroll	Fulfillment

Table 6.7 Systems/Criticality Spreadsheet

System/Criticality	Nice to Have	Optional	Essential	Mission-Critical
System 1	X			
System 2		X		
System 3			X	
System 4				X
System 5			X	
System 6			X	

Clicking on the second-level spreadsheet's system entries (**FIN SERVER, PAY SERVICE,** and **TM SERVER)** would take you to another spreadsheet that contained the specific information about that system. This could be configuration information, vendor information, warranty information, etc., or contact and account information for the services in use.

When you are done, you can choose to combine these spreadsheets into an enterprise-wide one that, instead of listing systems, lists business units. Where do you get the classification, criticality, and impact numbers? That's a bit tricky. Yes, you could theoretically apply a formula based on the individual business units' impact assessments, but you would be off. As I am sure you realize, any one business unit may have one or more systems scoring high on classification, criticality, and impact while the business unit itself would score low at an enterprise level. That is why assigning those numbers is best left to the executive management team and (if necessary) to the board. Your goal for that spreadsheet is to arrive at a prioritization by business unit for business continuity and disaster recovery purposes. This prioritization will filter down to your cybersecurity program work as you tackle the creation of an incident-response plan in case of a cyberattack.

You can also separate out different components of these spreadsheets for easier review and presentation. For example, you can separate out Impact and Criticality by creating an impact-specific spreadsheet per system. That table could look like Table 6.6.

Of course, as much as I wanted to put in *"CEO Blog"* as *"Mission-Critical"* with *"No Impact,"* I was advised against it, and left the entry blank. After all, how many mission-critical systems do you know that have no impact? (The rest of the examples are also to be taken with a grain of salt. Or two. Used only for demonstration purposes. Please don't send hate mail. Thank you.)

Another example of a table you can derive is shown in Table 6.7.

You can derive any combination you need, and many you don't: Criticality by Location, Impact by Asset/System, Resources by MTD. Each one can provide different insight on how to best manage the overall risk to the organization.

There is one more thing left to do. You need to assign a financial value to all of these assets (systems, and others) that you have so painstakingly cataloged, indexed, assessed, inventoried, and reviewed. Typically, this solicits the response: “Good luck with that!” Unfortunately, that won't suffice here. We need to get some sort of valuation in the books.

Now, before you start running for the hills, consider this: We're not really looking for a formal, accounting, audit-proof valuation. Sure, that would be very nice to have (and in some cases required), but we can make do with an informal valuation. You may also ask “Why now?” Why couldn't we do this as we spent all those hours of uninterrupted fun doing the asset classification and business-impact analysis work? Well, the truth is that you *could* do it then, but I recommend that you don't. Instead, I recommend that you take the opportunity to do a presentation of your findings to date to all those involved. This will give you valuable feedback (in case something was missed), and give them a unique view of their world as seen through your eyes. That is when I feel is the best opportunity to talk dollars and cents.

So, corral your business unit owners and executive team and don't let them leave the room until they give you what you need: a number per asset. Some sort of quantifiable dollar value that answers the question: How much is the asset worth to you?

Replacement value is an easy starting point for most executives to grasp. What would it take to replace a particular asset? Think about it holistically: purchase or lease, equipment, licenses, expertise, staff time, the works. It's not that crazy of a calculation, really.

When you're done with the first pass, let's talk damages. What kind? Which assets or units are affected? All? Some? Which contracts? What services? Any products? Any regulatory implications? What about reputation? You should assess those costs as well. For example, your team will know the value of the contracts and the corresponding penalties and losses associated with failure to fulfill. They also will know any regulatory penalties that may ensue as a result of a loss or breach. Finally, you can estimate with the team the cost of rebuilding the firm's reputation when those emails that you called people all sorts of names leak out. You got this!

That's it. Now, you're done. You added the last field on your spreadsheet: Impact, expressed in dollars. Take a well-earned break, and get ready for the next step.

Mitigating Risk

- Controls, as we discussed earlier, do stuff. You know the drill by now. They are *preventative* (think: Stop signs)*, detective* (think: cameras), *corrective* (think: backup), and *compensating* (think: failover sites). Now that you understand both your assets and the threat landscape, you can start making intelligent choices about which controls to apply to protect yourself. The goal to remember is: *defense in depth*. You want your controls laid out in layers. You want the ability to thwart an attacker at all the different stages of an attack, across various systems, and you need controls to mitigate all the vulnerabilities you discovered.
- The last factors to consider in developing your cybersecurity program are processes and—again—people. In a sense, we've come full circle: We started with people, and we are ending with people, only this time we're adding a crucial link. Processes. They are absolutely critical in your program's success. Processes are the essence of *how* business is done. They link assets, connect people, and create value. Some processes cannot be disturbed and must be protected as is. Others have more flexibility and can bend to accommodate controls.
- To find out which is which, you'll have to map all key processes in the company. This may not be fun, but it is essential that it be done and done correctly. Your work in this may brush up against bigger issues like overall information security, not just our favorite subset of cybersecurity. For example, consider a credit card processing workflow. It's not only the systems that need protecting. The whole process—from the moment your client gives you a credit card number to the moment the transaction is complete and filed—must be carefully thought out and appropriately protected. You may discover that you may need a different set of controls, which are not necessarily cybersecurity controls, to protect these mission-critical processes and people.
- People, of course, is what this is all about.
- People are the ultimate value creators, the true engine of creativity, innovation, and the spirit of your company. They are your biggest asset, and as such your top priority in ensuring their protection.
- People can also be your largest liability. They can be a liability if they are not aware of the threats, if they are ill-prepared to deal with the environment, or worse yet, if among them there is a “bad apple” who is intent on compromising everyone else's hard work.
- You can apply controls to protect assets and systems, but you cannot control people. That should not be confused. Ever. Interestingly enough, well-trained, sensitized, cybersecurity-aware people are the best way for the company to survive and thrive. That makes them one of your most effective controls, since through their training and awareness they actually do stuff to protect the assets! We will review how to develop the right cybersecurity awareness program in the chapters that follow.

- ## Incident-Response Planning

You may have heard of FISMA. It stands for Federal Information Security Management Act. It was signed into law in 2002, and it essentially requires all federal agencies to develop an incident-response plan.

I know what you're thinking—"But my company is private, so why should I care about federal regulations?" The reason is that similar legislation requiring your firm to do the same is probably not too far away. For example, New York State passed 23 NYCRR 500, a regulation requiring most financial and insurance firms to retain a chief information security officer (CISO), have a robust cybersecurity program, perform risk assessments and testing, roll out two-factor authentication, and report incidents within the first 72 hours. And, of course, develop an incident-response plan.

Why do I predict that such regulations are imminent? Consider seatbelts as an example. Once considered optional, the current policy on seatbelts is "Click it or ticket." Having an incident-response plan is like a seatbelt for your IT. It may not prevent an attack (that's what all the other stuff is for) but if one happens anyway, it will help limit the damage.

Another reason politicians are likely to get involved with requiring these plans is that insurance companies and governments are not prepared to shoulder the hits from an attack alone. And neither should you. You need the help.

The good news is that there are plenty of resources to help you develop an incident-response plan. The bad news is that developing an incident-response plan can be fairly complicated. In a sense, it's similar to building a hospital. The basics are obvious: You know it must have an emergency room, diagnostic facilities, intensive care units, operating rooms, patient rooms, offices, etc. But that's just the beginning! You also need to know the community that this hospital will be serving. Is it a metro area? Is it a small town? A group of isolated villages? Is the hospital in the tropics? The Arctic? And more questions follow: Who's funding it? The community? A wealthy donor? Is this a private company or government-owned? What kind of specialties will it have?

You get the idea. Your preexisting knowledge of minimum essential services plus demographics, geography, and budget will go a long way in deciding size and scope. For example, maybe your hospital can handle most everyday types of medical care, but when it comes to a body-part transplant, you'll need to refer the patient to a more specialized facility.

The same is true with your incident-response plan. Your firm's size, location, and budget will determine how sophisticated the plan will be. A small company may have an incident-response plan that calls for identifying an incident and immediately calling in outside expertise. A larger firm may have multiple incident-response specialists in house. As you can guess, the most critical step in developing your incident-response plan is going into it prepared to answer these questions.

Incident-Response Plan Phases

August 2012 was, for its time, a record breaker. Much warmer than average in New England, 63 percent of the states suffered droughts while Florida was getting drowned from Hurricane Isaac and a bunch of tropical storms.

Meanwhile, back in Gaithersburg, Maryland, the National Institute of Standards and Technology (NIST) was hard at work releasing *NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide*. You have to hand it to them; their titles are killers! But that's nothing compared to what's inside.

Currently, NIST 800-61r2, as it's known, is required reading for anyone in the cybersecurity field. It is a beautiful piece of work, and if you plan to get hands-on with incident management, you need to get intimate with it. You should also get real close with such other captivating titles like *ISO/IEC 27035-2 Information Technology—Security Techniques—Information Security Incident Management—Part 2: Guidelines to plan and prepare for incident response*. (No, I am not kidding. That's the title. Fantastic work, too.) And while you're at it, you should also consult *ENISA's Actionable Information for Security Incident Response, Strategies for Incident Response and Cyber Crisis Cooperation,* and *NCSS Good Practice Guide—Designing and Implementing National Cyber Security Strategies*. Can't wait for more? The list is long, and sampled in this book's bibliography.

What do you need to understand from all this? What are the essential elements of an incident-response plan that you need to own in order to complete your own cybersecurity program?

The first critical thing to understand is that incident response is a program in and of itself. As such, it has its own distinct phases, and much like the overall cybersecurity program, it, too, is a living program. It's not one and done; it's a continuously managed program.

What are the phases? Have you heard of Elisabeth Kübler-Ross's five stages of grief: denial, anger, bargaining, depression, and acceptance? Many people go through them during an incident: “No! This can't be happening to us!” followed by choice expletives, then by the desire to pay to make this go away, quickly replaced by depression about having to face the music, and finally acceptance of the fact that you, like millions of others, are a victim of a cybercrime.

But the core phases of incident-response planning are less gloomy. They are: preparing for incidents, identifying the occurrence of an incident, containing the incident, treating the incident (e.g., killing the virus, disabling access, etc.), recovering from the incident, and post-incident review, aka the lessons-learned phase. That last one is key and should never be omitted.

To properly prepare for an incident you need to have in place three things:

1. A business continuity plan.

2. A disaster recovery plan.
3. An incident-response plan.

The business continuity plan is the plan that the business has prepared to ensure continuity of operations and value delivery in case of disruption. A business disruption could involve a natural disaster like a hurricane, an earthquake, or disease outbreak. Or it could a man-made disaster like a terrorist attack or a cyberattack. It could even involve a simple human failing, like what happens when Julie from Accounting gets food poisoning from the cafeteria's tacos.

The business continuity (BC) plan has all sorts of useful information that feeds into the incident-response plan. For example, it has a defined business continuity organizational structure, policies, and workflows, as well as information about who can trigger the BC plan and how that occurs, detailed contact information, including emergency contact numbers, client and vendor information, relocation strategies, recovery procedures, and the like. The benefit of the BC is that if and when it is invoked, different parts of the business execute different workflows designed to protect people, communicate effectively with all affected, and initiate as rapid a business recovery as possible.

The disaster recovery plan (DR) is technology centric. Its focus is in recovering the technology infrastructure of the company. This is where you will find all our favorite acronyms and their values per system: recovery time objectives (RTO), recovery point objectives (RPO), and the maximum tolerable downtime (MTD). All directly influence the incident-response plan.

Consider, for example, if you have zero MTD. You'll recall, we've been there before, but it's worth repeating here: Who has such zero tolerance for downtime? Trading systems. Banking systems. Air traffic control systems. Utility systems. And, for some of us, Uncle Bob's Bagel and Pastrami Paradise. How do their incident-response plans address this requirement, keeping in mind that a cyberattack on a trading system may well have strict regulatory implications, which means preserving evidence, forensics, etc.? You would need to plan for a zero MTD *and* remain compliant to regulations, which means you can't just kill the intruder, reboot the system, and you're back in business. As a matter of fact, shutting down an infected system would wipe its volatile memory, destroying any forensic data that may be there.

Do you see now why planning ahead is so important? You need to take this a step at a time.

Preparing *Your* Incident-Response Plan

Notice the use of *your* as opposed to the generic incident response discussed earlier. No two IR plans are alike. They depend on many variables, from the size of the company (ranging from a small business to a multinational), to the scope of business, regulatory needs, and company culture. You might be surprised to hear that the last one plays a role in incident response, but it does. An active, engaged, and educated user community is an important asset in detection, in communications, and in remediation. A passive, disengaged, and generally cyberignorant culture frequently contributes to the incident and may even hinder its remediation.

By understanding your business-continuity and disaster-recovery plans, you will gain a solid footing in framing your incident-response plan. Similarly, the absence of either of these two plans speaks volumes about the company's priorities and risk management capabilities. It is your job to confront this reality head on, starting with engaging the executive team, whose active support is a requirement in all cybersecurity program development efforts, and critical in developing incident-response capabilities.

Remember back to our hospital-building analogy? All previous aspects of cybersecurity program development were akin to building the different wards and wings of the hospital. Incident response is the surgical center. Question number one, therefore, is: *Do you need a surgical center, or are you shipping your patients to a different facility altogether?* Otherwise phrased: *Do you need, can you afford, and will you keep engaged, an in-house incident-response team, or do you need to enter into an agreement with an outside incident-response provider?*

For the majority of small to mid-sized businesses, the answer will be to outsource the incident-response function (at a minimum). If this were a hospital, that would mean you keep the internists (or at least the nurses) in-house, but outsource the surgeons. It is highly unlikely that a small business will be able to both afford and to keep engaged a team of highly skilled and specialized cybersecurity incident-response people. But that doesn't get you off the hook from designing your incident-response plan! Remember, you can outsource responsibility, but you cannot outsource accountability. You still need to work with the service provider in designing and owning the plan. For your cybersecurity program development effort to succeed, you must always maintain accountability and full ownership. You are the one responsible for being knowledgeable enough and engaged enough to be able to successfully complete a cybersecurity handshake with your vendors.

For those businesses that need an in-house team for incident responses, you must also recognize that you will need to provide a complete ecosystem for them to succeed. They will need to report to the chief information security officer (CISO), and have access to the risk management teams, information technology, human resources, legal, and communications departments. The minimum size of an incident-response team will always be two: an incident-response manager and an incident-response engineer. One interfaces with the organization and directs the incident response while the other is deep in the weeds doing forensic and remediation work. The larger the organization, the larger the incident-response team and the more specialized and complex its structure.

Irrespective of size and scope of company, be it in-house or outsourced, your incident-response plan will need to address several key components, starting with a detailed description of your incident-response policies, standards, procedures, and guidelines. These, thankfully, will be derived to a considerable extent from your business continuity and disaster recovery plans, with the added input of at least risk management, legal, and communications. These policies will introduce organizational structure and will essentially define the *who-does-what-when* part of the incident response.

Regarding organizational structure, you'll need to adopt the one that best reflects the organization's needs. If you are decentralized, you may need decentralized incident-response teams. If not, perhaps a single centralized team is best. Depending on size and scope, you may decide to introduce a blended approach, where some incident-response capabilities are in-house while the rest are outsourced. This works well when there is a large headquarters-type of facility with smaller satellite offices scattered around the planet. In this case, you're probably better off having a centralized incident-response team at headquarters, with several vetted and contracted incident-response vendors at the remote locations ready to coordinate with you. All involved get a copy of the plan, typically saved in a big red binder with "Don't Panic" written all over it.

One absolutely critical part of your incident-response plan is a clear definition of communications protocols. Think of this as the *who-says-what-to-whom-when* part of the plan. This is key. For one, you don't want to instigate a panic among users by screaming through the speakerphones, "Incident Alert! Incident Alert!" And you certainly don't want to broadcast to the bad guys that you have detected an incident. So, avoid emails (they may have been compromised), avoid nonsecure messaging platforms, even unsecured telephone lines that may have been compromised. To the degree possible, stick with personal, one-on-one, need-to-know secure communications. Needless to say, this is not the time to get social! This is the time to carefully assess what exactly is happening, its impact on the business, on its clients and vendors, and, of course, the need to notify law enforcement and regulators. The last thing you want to happen is to have someone from the press calling you with, "I got a tweet about you folks having been breached.…Can you comment on that?" That's not a good place to find yourself.

The *whom* in the *who-says-what-to-whom-when* workflow can be long and dynamic. It will change regularly, and likely involve several third parties like your own insurance company, business vendors, cloud solutions providers, your Internet services providers, and a slew of information technology vendors and their incident-response teams. You may be required to notify law enforcement—my go-to is always the FBI and the local district attorney's office. If you happen to be a multinational, then the list becomes substantially longer since you may need to comply with local regulations on incident reporting country by country. On top of all these, you should consider sharing the information that you have with the United States Computer Emergency Readiness Team (US-CERT) and other industry-specific incident-response organizations.

The fun part of notifications, of course, is letting your clients know about the breach. To be clear: There is no avoiding this, and the experience will not get better with time. The last thing you want is to have your clients learn about the situation from the news media. You need to be prepared and well-rehearsed. Legal, insurance, and communications departments must all be in complete alignment on (at a minimum) what happened, who did it, why it happened, what you are doing in response, and how you're making sure it will not happen again. You may not know all the facts (e.g., who's behind it), but you need to be as proactive in your communications as due care and prudence will allow. Nothing destroys trust in a company faster than a poorly communicated cyber-incident. Get in front of it as soon as is practical—engage the news media and be as forthcoming as possible.

The next step in your incident-response plan creation is to integrate the wonderful results of your work to date in threat analysis, environments, and defense-in-depth and control deployments. The plan needs to reference all these, with specific clarity on where your threat intelligence is coming from and how you can leverage that in case of an incident, your environments at risk (clouds, Internet-connected devices, and your distributed workforce), and your defense-in-depth and controls deployments. These will be critical in both the detection of an incident and the response to it. Remember, all these entries in your plan need to be kept current. All this is dynamic, and for the plan to be useful, it needs to reflect the appropriate level of changes over time. What does this mean for you? Get comfortable with two words: change management.

To complete your incident-response plan, you will need two more entries. First, you will need to identify your incident-response toolkit. This is a set of mostly software tools (there are some hardware tools as well) that are specifically built for forensic and incident-response work. *Please note: These are surgical instruments, and they need to be handled by experts*. Moreover, the toolkit, like all else, evolves over time; in fact, toolkits are the fastest-evolving component of your response, because software is constantly updated. It is therefore critical that the plan reflect the most up-to-date toolkit in use, its locations (yes, there needs to be more than one), and any access credentials necessary. You do not want to be scrambling for USB keys in the middle of an attack. You need to know where your toolkit is, what is in it, and who are the right people to use it.

I can't emphasize enough the importance of the right people. Forensic and incident-response work is very complicated and requires highly skilled specialists. Even the best-intentioned and expert IT professional can wreak havoc if she attempts to use forensic tools without specialized training and experience. There are any number of case studies where IR professionals walked into a site under attack only to find the well-meaning IT team having turned off the servers and already restoring systems from backup. This common mistake destroys the evidence, leaving you with no way to know who attacked and why, no way to learn how to prevent it in the future, and so on.

The last component of your incident-response plan is the training. And by that I don't mean the company-wide cybersecurity awareness training I discussed earlier. Here I mean war games. Full, all-out, incident-response exercises, conducted frequently and analyzed exhaustively. Just like the old joke about how do you get to Carnegie Hall, the only way to get to be good at incident response is practice, practice, practice. The higher your dependence on your IR team, the more and rigorous your practice exercises must be—think Red Teams and Blue Teams; the works! The exercises need to be comprehensive across all your environments and include your executive team, staff, and all key vendors. Some should be well planned, rehearsed, and announced while others should be out-of-the-blue surprise drills. Everyone, from executives on down, should be aware and sensitized to incident response. They all have a role to play.

Meanwhile, your IR team should never rest. I know, it sounds harsh and too much. But, that's the job. It's what they do. Constant training and practicing is the only thing that will make the final difference during a real attack. Now, get to it!

Identifying Incidents

Armed with your up-to-date, shiny, fire-engine-red, “Don't Panic” folder, you're ready to exercise your incident-response plan. All you need is an incident! If you're lucky, you'll wait for a nice, long time, giving you all the training opportunities, your team needs. If you're not…

How do you identify an incident? You monitor your environment. And by that I mean 24 × 7 × 365. Every system. Every action. Every event. Monitor. Monitor. Monitor. For the average company, monitoring will produce several thousand lines' worth of log entries and alerts from half a dozen systems (servers, firewalls, antivirus and antimalware software, switches, end points, etc.) or more. If your company is an above-average technology consumer, you will be dealing with potentially millions of log entries and events. Attempting to correlate all this, much less make sense of it all, is not something humans can manage on their own.

To be clear: Identifying an incident is far from trivial. Many have gone undetected for weeks and even months! It's not about interpreting alerts, reading logs, or processing user feedback. Hundreds of events in the course of doing business can be mistaken as a security incident. An application may modify a configuration file, and you get an alert: Is it an incident, or a normal function? A file server is slow: Incident, or just a heavy traffic load? Access to the Internet is spotty: Incident, or ISP errors? A file modification alert has been issued: Malware, or normal use? You received an email with a threat alert. Is it mere spam or a sign of things to come? Unfortunately, all these will need to be looked at through your cybersecurity glasses, even if they end up being little else than routine bugs.

Enter SIEM. Security Information and Event Management systems ingest all this information (logs, threat feeds, etc.), correlate it, and issue alerts about abnormal events in your environment. What's not to love? Nothing. Except that not all SIEMs are alike, and, like all relationships, you need to put work into it to get the benefits out of it.

First, you should do your due diligence and select the right SIEM for your environment. They come in all sorts of sizes and flavors, including SIEM-as-a-service options. Second, depending on which system you deploy, you may have to fine-tune it. Make your SIEM too paranoid and every alert issued becomes a ticket to be investigated. But tune it to apathy and you won't be notified until your data center has been pounded into fine silicon dust.

Once tuned, a good SIEM will be your best friend and cybersecurity partner. You'll be working hand in hand in processing the alerts, creating tickets, documenting trends, correlating with threat intelligence, and escalating to containment and treatment. All this beautifully orchestrated work will also be feeding into your cyberdocumentation tools, which your reporting workflows can use to notify authorities, incident information-sharing organizations, wikis, and late-night glee clubs.

The catch, of course, is that to reach this level of incident-detection bliss will require not only the right, and properly configured, SIEM choice and the right systems management practices (e.g., documentation, normalization, synchronization, etc.), but the right defense-in-depth strategy to begin with, which—you will recall—is the one that resulted in the deployment of the right controls that are being monitored across your environment in the first place.

And how did you get to the right defense-in-depth strategy? You got there because you did all the hard work during the asset, threat, vulnerabilities, and environments phases.

Who's better than you? No one, that's who!

Containing Incidents

ALERT! ALERT! This is not a drill!

You have an alert that was identified as legit, was pressure tested, checked, and escalated to containment. Something is truly up! Now what?

Step one: Heed the advice on the front of your binder! *Do not panic!* You've got this.

Step two: Identification. What are you dealing with? What are your detective controls telling you?

Step three: Analysis. This is elbow-grease work requiring unique skills and specialized tools.

Step four: Action. Once you know *who, how,* and *what,* you need to be ready to take action: Do you want to maintain the evidence for possible future actions (for example, prosecution)? Do you want to get back to operations as soon as possible with little regard to evidence preservation? Do you want to tolerate the infection while you develop workarounds? These are decisions that you should have thought out ahead of time and practiced with both your incident team and your top-level management.

Let's look more closely at step four, action. To properly contain the incident, you'll need to know three things: *who, how,* and *what*.

1. *Who:* Who is behind the attack? Is this an accident? Is this an insider? Is this an act of terrorism? What do the threat feeds say about who's behind it? What is the motive? Understanding the *who* will help you develop methods of containment and treatment.
2. *How:* What is the attack vector? Malware, and if so, which kind? Is this the result of a virus? A Trojan? A worm? Did someone plug in an infected USB somewhere? Did someone click a link on an email? Was this a "drive-by shooting," such as malware dropped on a computer while someone was just browsing? Or was the breach perhaps the result of stolen credentials? It may

be one or more of these things, or none of them. There could be some entirely other, more unusual way that the attacker used to compromise your systems. Your team will need to identify the *how* in order to contain it and potentially identify ways to preserve forensic data.

3. *What was hit?* A single end point? Multiple ones? Servers? Applications? Networks? Your forensic people will need to do a detailed end-point analysis on the affected systems to collect evidence. This will include any kind of tracks that the attacker left behind, including a bit-by-bit copy of what is in the volatile memory (not just the permanent storage [e.g., hard disk, SSD, etc.]). They will need to establish the incident timeline: When did the attack start, how did it propagate, what did it leave behind, what are the effects? Part of this process involves highly technical work that may include isolating the malware on a system for observation, or reverse engineering the malware to understand what the code is doing. Once all this is understood, then all systems across the company will need to be forensically verified that they have not been infected as well.

It bears repeating that in the incident-containment phase, knowing what *not* to do is as important as knowing what *to* do. If your company does not have the resident expertise, a panicked executive, or IT person being flooded by alerts, may be tempted to pull the plug of the infected computer, try to use some I-got-it-from-the-Internet-malware-removal-tool, or—worse yet—log in as the administrator to investigate it or call your friend in the FBI.

This is why it is so critical to have a plan in place before the incident, and to practice, practice, practice! Knowing what to do and how to do it gets you half-way toward resolution.

Treating Incidents

When it comes to treatment, I have bad news and bad news. First, the bad news.

Sometimes, you may have to live with the disease. You may need to live with it because of critical business considerations that prohibit you for isolating or rebuilding one or more systems. Or, you may need to keep the infected systems running so that the attackers don't realize that you are aware of them while shielding more valuable assets, or sending Delta Force over to kick in their doors. Similarly, there may be upstream or downstream dependencies that require you to get creative. For example, because of business requirements of nonstop use, you may need to restore the infected system onto brand new hardware and then reinsert it into production while taking the infected system out. That can prove about as easy as replacing an aircraft engine while it's in flight. It's doable but very, very windy.

Other times, you may be required to preserve the infected systems for evidence. That's all fine and good if you have one server that's infected; it's a whole other story if you have 50 of them sneezing and wheezing with a virus. Complicating things further is virtualization. These days, you can have multiple virtual computers running on one physical one. Despite ironclad assurances from virtualization vendors that there can never be cross-contamination across virtual machine boundaries, I remain a skeptic. I am a firm believer that if one person can build it, another can break it. So, I would not be surprised if a virus was created that could jump the virtualization boundary, despite whatever assurances you've been given. Remember, everyone lies.

Finally, after evidence has been preserved, requirements have been met, all the *t*'s crossed and all the *i*'s dotted, there is the fun part of coordinating one or more infected systems. Not only do you need the incident-response team on the same page, you need the whole organization to know that the following systems will go offline, for how long, what the impact may be, and so on and so forth. Depending on the number of systems, this can be an expensive, resource-intensive exercise. Plus, you'll make a whole new set of friends when you announce that all the passwords have been changed.

Which brings us to the bad news.

The only way to ensure that an infected system has been cured is to go to bare metal. This means that you need to completely and thoroughly wipe the infected system and rebuild it bottom-up from clean installation media. There is no sugarcoating this. If you need to be 99.99 percent sure that the infection is gone, the only way to do it is by burning the box and reinstalling everything new.

Why only 99.99 percent sure, even after a clean wipe? Because, word on the street has it that some agencies have developed malware that infects the actual hardware itself. Allegedly, this type of malware can infect the BIOS (basic input/output system) of a computer, or certain EPROM (erasable programmable read-only memory) chips, such that even after you wipe the computer, the malware can reinstall itself.

Of course, even wiping a single system is a time-consuming exercise. Not only do you need to have the clean installation media at hand, you also need to account for configuration settings, clean backup availability, data synchronization when the system gets reinserted into production, etc. Now, multiply this times the number of infected systems. This is where your disaster recovery planning will shine. Having clean, recent, whole-image backups per system will go a long way toward a rapid recovery.

Incident Recovery

With the incident treated, you are ready to bring your systems back online. There are several questions that need answering here, bridging the incident treatment process and final incident recovery.

First, way before any incident, you must have considered the need for evidence preservation. If you are required to do forensic preservation, then you cannot wipe the infected equipment and rebuild. You'll need replacement gear. Moreover, the documentation needs and requirements for evidence preservation are extensive. Your team will need to be familiar with all the laws and requirements for evidence handling, chain-of-custody documentation, proper evidence gathering. Your best bet is to retain a forensic firm to help you. They will interface with your attorney and your incident-response team, and make sure that all the evidence is taken care of properly.

Second, your incident-recovery strategy hinges on your known values of MTD, your maximum tolerable downtime, the RPO, your recovery point objective, and the RTO, your recovery time objective. You have documented all of this before any incident, and they have governed your disaster recovery strategy. Here and now is where all this will be tested.

As with all things, recovery from an incident will fall on a spectrum. There will be companies whose MTD is practically zero and will therefore have hot failover sites, air gapped (i.e., non-Internet accessible) backup and archives, and multi-timeline mirrors (mirroring strategy and the necessary equipment that creates isolated versions of mission-critical systems over predefined timelines—for example a real-time mirror, a day-old mirror, a week-old mirror, a month-old mirror, and so on). Those companies will be using an army of resources to recover, because that's what it's worth to them, and frequently *is* what is required of them (think utilities, national security installations, water purification, air traffic control, etc.).

Then, there are the majority of companies that can afford an MTD of hours or days. Their strategy is more appropriate to that timeline, meaning that your team has some runway to be able to restore systems to production. That is not to say that there is a company out there that doesn't want the absolute minimum MTD. This is to say that the majority of companies are smart enough to not overpay for disaster recovery when they can tolerate a few days' worth of an outage. There may be a question about if those smarts are developed from proper risk management–centric thinking, or from “Are you crazy? I am not paying all this money for backup!” reactions. Either way, most IT departments have in place a budget-appropriate solution that has been implicitly accepted as appropriate.

Lastly, there are (hopefully) a minority of companies that have not thought through any of this. For them, incident recovery is…challenging. Some may never recover and go out of business (consider malware that destroys all data in the absence of a backup). Some will pay a dear price in both time and money and get only a partial recovery. Either way, if you are reading this book, and you're this far in and have realized that this paragraph describes your company, you have a lot of work to do, and you'd best hurry up!

In our case, I am confident that you have evaluated and vetted your disaster recovery strategies and solutions as appropriate to your risk appetite, cybersecurity exposure, and so on, so we'll accept that your environment falls squarely into the smart group of companies! While your team is restoring your production environment, you are making sure that they are following a pre-rehearsed checklist that affirms proper and normal operation of all systems, following the communications and notifications protocols, and all departments are working together in incident-response harmony. At the same time, you are making exhaustive notes on the incident that will help you in your post-incident review and action plan.

Post-Incident Review

There will be *incidents* and there will be *INCIDENTS!* Both will require your careful review. People call post-incident review many different things (lessons learned, postmortem, etc.), but no matter what you choose to call it, the review process is essential to the evolution of your cybersecurity program and team skills. To begin with, you need an answer to a whole list of questions, starting with:

- *Who's responsible for this outrage?* You should be able to answer this with confidence. And yet the question is more complex than it seems. It's not about merely assigning a name to the attacker; it is about building a complete profile. Sometimes getting a name will be impossible. You will still be able to glean quite a bit from the tools used, origin, threat intelligence feeds, and plain old Internet searching. Try to build as good a profile as possible. Understanding your attackers, their motives, and their methods will help you prepare for the next attack.
- *Just the facts, ma'am!* After the *who,* you need to document the *how,* and you need to do it in excruciating detail. You need to know exactly what happened, when it happened, how it happened, what vulnerabilities were exploited, how it was discovered, which alerts were triggered, and which were not. You need all the facts about the incident, in as much detail as possible. This will help you tune your defenses and identify holes in your control deployment.
- *Knowing now what you didn't know then, what do you need to change?* This is the introspective component of the exercise. You need to look inward and understand how your organization reacted to the incident. Look at everything and leave no stone unturned. How did the incident-response team act? Were procedures followed? Were internal communications effective? Was the response time adequate? Were the response actions timely and adequate? Did you meet MTD, RPO, and RTO targets? How did the executive team support the effort? How did the staff react? How was the IT-cybersecurity partnership performance? Once these questions are answered, you can collectively sit down and tune your incident-response plan such that next time you can perform better.
- *How do you stop this from happening again?* Having understood the organization's and team's performance, plus all about the incident itself, you need to plug the hole that allowed the incident to occur in the first place. This sounds a lot easier than it is. If the breach was due to a phishing incident, for example, your options may be limited to better email sandbox tuning and targeted cybersecurity awareness training. Neither of those will plug the hole completely. They may narrow it, but there is no guarantee that another member of the staff will not fall victim to such an attack. In which case, you're going back to layered defenses (sandboxing, role authorities, monitoring, training, etc.).

Do It All Over Again!

As we discussed earlier, cybersecurity program development in general and incident-response planning specifically are living programs. They change over time, they change with your environment, the market, the technology, and they change because you change. You learn, you grow, you adapt.

The good news is that as you learn, grow, and adapt, you can apply your knowledge, experience, and adaptation to your cybersecurity and incident-response plans. You get a second chance! And, a third, and a fourth….

Change is the only constant here, and it represents a wonderful opportunity in keeping your cybersecurity program constantly tuned. Embrace this, and take advantage of it. The alternative is catastrophic: An obsolete cybersecurity and incident-response program are just as bad as not having any.

Based on your earlier definition of cybersecurity and taking into consideration the CIA triad, defense in depth, and that to assess risk you need to address all systems, people, and processes, explain why:

People are the most effective controls in cybersecurity

Remember our initial definition of *cybersecurity? Cybersecurity is the ongoing application of best practices intended to ensure and preserve confidentiality, integrity, and availability of digital information as well as the safety of people and environments*.

And, of course, the triad from our defense-in-depth discussion? *People, technology,* and *operations*.

Finally, which is one of the most effective controls in cybersecurity? *People!*

People, people, people! You may say I revel in stating the obvious, but all the work we've done so far is not about data, assets, or some document that defines a corporation. It is only about people. I've emphasized this in every chapter: Our work, your work, is people-centric.

People, it bears repeating, are at once your biggest asset and potential liability. As assets, they create value, they align with goals, and help protect the values they create. As liabilities, they can just as easily destroy these values through lack of awareness, carelessness, or ill will.

Your challenges in creating your cybersecurity program are twofold: First, you are creating a program for your people. Second, you must engage the same people to make the program a success.

That last one is trickier than it sounds!

Senior management approval for the cybersecurity program is paramount

For any cybersecurity program to succeed, no matter its scope and delivery method, you must secure the vocal participation of your leadership team. They need to advocate for it, they need to participate in it, and they need to evangelize their middle managers on the importance of it.

We need the right message to motivate the company

Back in 1951, Professor Carl I. Hovland and Walter Weiss of Yale University delivered a great paper, “The Influence of Source Credibility on Communication Effectiveness.” It is in that paper that we learn that subjects, at the time of information exposure, discounted material from “untrustworthy sources.” The problem is that with time, the same subjects tended to disassociate the content and the source, resulting in the acceptance of…Fake News! As a matter of fact, Hovland and Weiss discovered that “lies, in fact, seemed to be remembered better than truths.”

As fascinating as this is, even more interesting is what happens with the retention of the message, depending on the source, over time. They discovered that although a message from a highly credible source had a higher percentage chance of being initially accepted, its acceptance dropped substantially over time (as short as four weeks). They also discovered that the reverse is equally true. A message from an untrustworthy source had an initially smaller chance of being accepted, but over the same amount of time, its chances increased, eventually exceeding that of the trustworthy source.

Why is all this important to our cybersecurity program's success? Because the messenger matters just as much as the message. And because you may have to dislodge false, entrenched beliefs from people whose cooperation is essential to the program's success.

For example, if your CFO is absolutely convinced that there is no way that your company is on any hacker's radar, you'll have a very hard time trying to get funding for the cybersecurity program. You will need to shift the CFO's attitude, and to do this you'll need to use language and tools that she, and she alone, can understand. This needs to be a very individualized communication, with a specifically tailored message, delivered by the right messenger.

Here's the vital point: Sometimes, the messenger cannot be you. If everyone in the company knows you're the one pushing for the adoption of a cybersecurity program, the staff may feel that you're coming to the table with a specific point of view, trying to shove a program down their throats. Your goal of adoption may be best served by using an ally as the messenger. Pick a well-liked manager, or the business team members who have helped you along the way, or even independent consultants as your authoritative messengers. Stay focused on message adoption, not the messenger.

For a message to be adopted, it must have certain qualities. Those include being:

- *Succinct*. If your message is more than a few sentences, it's too long. Edit it down to your specific point. One point per message. Don't ramble.
- *Specific*. The message needs to be as specific as possible and it should obey the communications principle of who will do what by when. (If you need more on that, look no further than the book by Tom Hanson and Birgit Zacher Hanson titled *Who Will Do What By When? How to Improve Performance, Accountability and Trust with Integrity*).
- *Meaningful*. Why does this message make sense to the recipients? How is it pertinent to their work life?
- *Authoritative*. What's the associated authority issuing the message? In other words, why should we listen to you?
- *Doable*. At the end of the day, your message must reflect a call to action that can be achieved. It cannot be aspirational or shoot for the stars. It has to be achievable by the message recipient in a reasonable amount of time and through reasonable effort.

By understanding your audience and understanding both the power *and* the limitations of your message, you can frame your internal communications accordingly. More importantly, you can use this information to tailor your cybersecurity-awareness training to the specific strengths, weaknesses, and culture of your company.

Cybersecurity-Awareness Training

Just as no two cybersecurity programs are exactly alike, so it is with cybersecurity-awareness training programs. There are common elements, of course, and we'll examine them further on in this chapter. But you should never lose touch with the individuality of your company's culture and the specific needs of your people.

There are several ways you can conduct cybersecurity-awareness training. Your choice will depend on the size of the organization, the level of existing awareness of the topic, and your risk and threat assessments. Speaking of assessments, an excellent way to establish a training baseline is by doing a skills assessment on cybersecurity. This could be as easy as a fun quiz, or even an interactive game that you can push out to everyone's computer. The results will be instrumental in designing the training.

The following links represent my top general assessment cybersecurity quizzes. They are not as extensive or customized to any organization, but they certainly can help you get an overall sense of where your company's population cyberunderstanding is.

They are (alphabetically):

1. European Cyber Security Month (recurring, sponsored by ENISA and the European Commission) awareness campaign: https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/

2. FBI's “Cyber Surf Islands” games, especially made for students: https://sos.fbi.gov/?came_from=https%3A//sos.fbi.gov/welcome-fbi-cyber-surf-island-fbi-sos-internet-challenge-text-only/
3. Federal Trade Commission's Phishing Scam “Avoid the Bait” quiz: https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/games/off-site/ogol/_phishing-scams.html
4. Khan Academy's Cybersecurity Quiz: https://www.khanacademy.org/partner-content/nova/cybersecurity/cyber/e/cybersecurity-101-quiz
5. Media Smarts: Canada's Centre for Digital and Media Literacy Quiz: http://mediasmarts.ca/sites/mediasmarts/files/games/cyber-security-quiz/index_en.html
6. Microsoft's “Test Your Cyber Security IQ”: http://www.microsoftbusinesshub.com/internet-security-iq?CR_CC=200682284
7. Pew Research Center: Internet and Technology, Cybersecurity Quiz: http://www.pewinternet.org/quiz/cybersecurity-knowledge/
8. SANS Cyber Aces Courses and Quizzes: http://www.cyberaces.org/courses/quizzes

Once that's done, you need to decide which training strategy is appropriate to your audience. Is it going to be a trainer-led program or a learner-led one? In the first case, the trainer is in control. He or she presents the material, the learners participate to the degree that the trainer allows, and they may be subsequently tested. In the learner-led approach, the learner is in control, the training material is consumed asynchronously (people learn as they want and when they want), and the trainer's role becomes that of a facilitator and guide as the learners navigate the material at their own pace and share their experiences.

In some cases, the strategy is dictated by the size and geography of the company. For example, it will be very difficult to have an instructor-led workshop for a company with a few hundred employees distributed all over the country. Similarly, an intimate “lunch and learn” may be all your company needs to start on the cybersecurity awareness path.

Once you have identified the needs and arrived at a training strategy, the next step is to pick the best way to deliver the information. Your choices include:

- *Presentations*. Whenever I do a presentation, my second slide is a famous *New Yorker* cartoon by Alex Gregory. In it, the devil is interviewing a torturer, and says, “I am looking for someone well versed in the art of torture—do you know PowerPoint?” The point is well taken. You can certainly use presentations to deliver cybersecurity awareness training, but be certain to be as engaging and inclusive during the training as possible. Otherwise, you run the risk of the glazed, sleepy-eyed, disengaged audience. My recommendation is to use presentations for what they are good for: Deliver specific guidance to a specific targeted audience. Keep them short. Keep them to the point. And be sure to keep them interactive.
- *Lunch and learn*. This is a less formal presentation. If at all possible, avoid slides and the like. Set up the room in as round and inclusive a layout as possible (no podium, be part of the audience). Your goal is to have a discussion about a cybersecurity topic over lunch. Any material for your learners should be handed to them at the beginning, and let them peruse them at their pace. Keep the topic focused. For example, you don't want to have a “Cybersecurity Awareness Lunch

and Learn." Be specific! You want to have "Phishing, and all the ways you can get hooked!" lunch and learn.
- *Group learning*. This is a great way to convey complex topics to either a small group, or sets of groups. For each group, you will need a skilled trainer in team-building and role-playing methodologies. The idea here is that you are taking a topic and really acting out everything there is to know about it. For example, if you're group learning about phishing, you may want to guide the group through an exercise in which members of the group alternate into the role of the hacker and try to fool the others to act on their instruction. What's the instruction? It can be anything, such as handing over a bunch of Legos! (Legos are a great interactive training prop! Don't leave your office without your Lego bucket!)
- *E-Learning*. If you have decided that your training strategy is a learner-led one, then e-learning will play a crucial role in successfully delivering and testing your cybersecurity awareness program. To be sure, e-learning can, and should, complement *any* training methodology. It allows for constant assessments, reminder quizzes, and on-demand availability of information. It also reinforces all the other methods, since it can be a complementary resource to those who want to know more about the specific topic, or for those who for some reason or another couldn't attend the instructor-led training.

The need for a Cybersecurity-Awareness Training program

There are several excellent e-learning cybersecurity awareness programs. Consider, for example, the SANS Institute training offerings, Inspired Learning, Wombat Security, PhishMe, and Security Mentor to name only a very few. Please note that this is not an endorsement of any of specific program, and the preceding list is far from complete. I am mentioning them here to start you on a path to discovery for the right vendor for your specific company needs. Do your research and due diligence, and partner with the vendor that is right for you.

I cannot emphasize enough the importance of integrating your specific company culture and needs with cybersecurity awareness training. It also goes without saying that this is not a one-and-done type of activity. Depending on size and scope of your company, you will need to provide regular refreshers, training support, quizzes, reminders, and so on. Also remember that you need to integrate the training across the life cycle of all employees—from onboarding to offboarding.

Be sure to include in your training their at-home behavior. Your employees are exposed to cyberthreats both at work and at home. After all, if an employee uses the same laptop at home as in the office, then the cybersecurity risks don't stop at the office door.

The good news is that a successful cybersecurity awareness program can be one your most effective controls in your defense-in-depth strategy. Companies with an aware population have seen up over a 30 percent improvement in their ability to detect phishing scams, insider threats, even abnormal system activities.

My advice: Take cybersecurity awareness training very, very seriously. Just because it is a soft control (as opposed to all the high-tech hardware, software, and services ready), that doesn't mean it's any less effective. As a matter of fact, time and time again, security awareness consistently proves itself as one of the best controls against attacks. Invest in it accordingly.

How to live cybersecure

Cybersecurity is a science; a hard one at that. A science that's rapidly evolving. New discoveries, new approaches, new best practices are discovered, tested, and applied daily. Staying on top of this field is no easy task—some would argue it's impossible—but staying informed is something that you can, and should, do. As we've discussed, cybersecurity is a shared responsibility, and staying on top of it is one of the things that you must do.

When it comes to staying on top of things, how much is enough? Much depends on your role and day-to-day responsibilities. For a busy C-level executive, receiving pertinent alerts and a weekly summary may be enough. For a hands-on operation executive with cybersecurity oversight responsibilities, a daily briefing may be necessary. For a board member, alerts and a quarterly report from the CISO may be all that is needed. Frequency, quantity, and context will be determined by the size and needs of your specific organization. One thing is certain: You will need to stay informed and current. Forever!

What else do you need to know? Well…that list is long. Very long!

What else do you need to know to support your newly created cybersecurity program? Now, that's more manageable, and I have some ideas!

In general, the things you need to be aware of tend to fall into one of the following categories:

- *Scientific developments*. These are straight-up developments in the field. Like I mentioned, there are thousands of cybersecurity professionals who are constantly pushing the envelope. Their dedication and breakthroughs are what makes this world a safer place, and books like this possible. Regarding where you can learn about their constant progress, my recommendation is to join one or more of the several worldwide organizations who support and advance the science and application of cybersecurity. For example, I have made frequent reference to CIS, ISACA, ISSA, (ISC)^2, ISO, and the SANS Institute. There are also government agencies like ENISA and NIST that also provide a wealth of information and best practices for a variety of industries and company sizes. A bit of research (and some well-spent membership dollars) will go a long way toward keeping you informed.
- *Regulatory developments*. These are typically legislative actions affecting cybersecurity implementation, and they can range from compulsory to strongly suggested. You certainly need to know about them—ideally, long before they're enacted—and plan accordingly. Moreover, you need to know about them everywhere in the world that you do business in. (See, for example, the European Union General Data Protection Regulation in Chapter 10.) You should expect regulatory actions at every level: city, state, and country. Whether your board, or

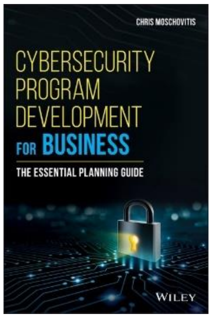
whoever accepts risk in your company, chooses to comply is another matter. Yes, noncompliance is an option. Remember: If the cost of a control is higher than the asset it is meant to protect, then it doesn't make sense to implement it. Therefore, if implementing a regulation is going to cost the company so much money and time as to not be worthwhile when compared to the fine, then it may make sense to pay the fine. To be clear: I am not advocating that you take this position; but I would be remiss not to alert you to it!

How do you get to find out about all these possible exciting developments? Typically, your industry-specific publication keeps track and reports on legislative developments that may affect you. That said, there is no substitute for staying informed about what your government representatives are doing. Get involved and stay involved. Start with a reputable major daily newspaper, and graduate to picking up the phone and calling your representative with any questions you may have. After all, it's your business we're talking about here.

- *Information technology and computer science developments*. These developments are many, constant, and far-reaching. We're not talking business disruption here. We're talking life-changing discoveries and developments that will forever change the way we work, think, communicate, learn, influence, and behave. Aside from Moore's law that, in essence, predicted the doubling of computing power every couple of years, there have been breakthroughs in artificial intelligence, machine learning, pattern analysis (think big data), blockchain technologies, and the integration of computing and communications capabilities into everything from a toaster oven to a pacemaker. Why do you need to know about this? Because, as we've discussed, these things will dramatically influence your workplace, and since you're the one sensitized to the cybersecurity implications, you also get to be the one who needs to get in front of these developments and—at least—think about their potential impact to your program, if not your life. How can you stay informed on these changes? At a minimum, I would recommend subscribing to MIT's *Technology Review,* the *Harvard Business Review,* and at least one industry-specific publication. Are there any other publications that are reliable sources of this type information? Absolutely, and by all means, subscribe to them all! The important thing here is for you to stay continuously informed.

Taken from:

Cybersecurity Program Development for Business
By Chris Moschovitis


CHRIS MOSCHOVITIS
CYBERSECURITY PROGRAM DEVELOPMENT FOR BUSINESS
THE ESSENTIAL PLANNING GUIDE
WILEY

PUBLISHED BY: Wiley

PUBLICATION DATE: May 2018