CHAPTER 4

Roles and Responsibilities

We are doing a bad job of drawing the line on what is and is not the responsibility of cybersecurity professionals, services, and products. If we continue to fail to understand ourselves and our roles and responsibilities, we cannot hope to innovate on how to improve. Cybersecurity should be defined as the protection of data through transit, processing, and storage, but there has been a large drift away from what true cybersecurity is and how it is employed. Cybersecurity has become all-encompassing in private business, throughout the government, and in our personal lives.

You hear the term everywhere and everything that beeps or squeaks now falls under the umbrella of cybersecurity. With everything now being connected or the Internet of Things (IoT), the area of responsibility now being levied on the cybersecurity professional is becoming unsustainable both fiscally and technologically in providing the protection in the areas truly needed. We must ask ourselves if we are inviting more risk and a larger attack surface all for connivance and appeasement of the employee to stay connected.

Just by looking at the devices that are now permitted if not issued in the workplace, it is easy to see how the cyber footprint has grown tremendously. These added devices, be it laptops, tablets, or smart phones, are often allowed to leave and connect to other networks and then return and reconnect to the company's managed network. This

J. G. Oakley et al., *Theoretical Cybersecurity*, https://doi.org/10.1007/978-1-4842-8300-4_4

simple and now wildly accepted practice is the responsibility of your cybersecurity professional to manage and defend. Even if these devices are company-owned and managed, it is added time, expense, and human capital to manage and protect these devices. This same problem exists with the bring your own device (BYoD) to work programs if it doesn't bring more risks to the company. It must be asked why it is now so widely accepted to introduce so much risk to a network for the possible increase in productivity from those who use these devices.

If productivity is the driving factor for BYoD and the issuing of digital devices to employees, then it must be weighed against the cost it will incur for supporting those decisions. The cybersecurity team will now have to draft a policy for end users' agreement, identify tools and techniques for scanning reporting. The team will now have to expend more man-hours to secure and defend all the extra devices in the name of productivity. There may be added cost of new software and licensing depending on existing licensing and tools used by the team. How is productivity measured for using these devices? Is it the number of emails received and responded to? Or is it by word count on documents created while not connected to the company's network?

Responsibilities to Shed

It is important to note that the medium through which a security or disingenuous act is precipitated through is not necessarily the reason it happens. As an example, think back to the by-mail scams of the 1990s wherein alleged royalty of other nations promised wealth in return for a tiny bit of help. This has become a notorious and meme-worthy scam where the victim offers a check or cash or money order to help this royal get out of their country or somehow otherwise obtain their new inheritance or wealth. Plenty of people fell for this scam and sent money or wasted time and effort trying to get the bigger pay day on the other end of the scam, which never came.

Now, this scam was facilitated through the US Postal Service (USPS). The inherent trust in something delivered to your mailbox by a uniformed governmental official lent credence to the contents of the scam letters and was undoubtedly part of what enabled them. However, no one would argue that this was a form of mail-attack or a mail-security issue. Why is it that when someone accomplishes the exact same scam through email that we call it a cyberattack or cybersecurity issue? The USPS certainly didn't offer up any responsibility for what you or the scammer did across its communications medium (the mail).

This is a bit of an oversimplification, but it paints the picture clearly on why there are certainly malicious activities taking place through the cyber domain that cybersecurity professionals are at best, overextending themselves by being on the hook for mitigating. At worst, this gives the perception that cybersecurity is not working in instances where it has not even been allowed input to a situation. Without shedding such examples, cybersecurity innovation and theory will be hard to foster due to overextension and widespread misconception about what cybersecurity should be and should focus on. The following are both real and fictitious case studies that illustrate several other areas where cybersecurity should shed its responsibility and rebuff attempts to include such activities in its purview. This is not exhaustive, and there are certainly more; the point to be taken is that an examination of what is and is not a cybersecurity issue must happen for theoretical cybersecurity to thrive.

Case Study 1

Mirroring similar real-world examples of fraud, in this case study, our victims had millions of dollars in crypto currency stolen from their account by ultimately putting themselves in a position to reset a crypto-wallet user's password and logging in to their account and transferring out funds.

What Happened

The thief (I am not saying hacker) took publicly available emails of senior executives of a crypto-wallet company that were published to that company's websites and used them as logins. The phone numbers of those individuals were found through simply looking them up on professional networking websites. The thief then went to the crypto-wallet user site, where at least one of these senior executives surely had an account (they admitted to using their own wallet service on both their website and professional networking profiles to lend credibility to it).

On the crypto-wallet site, the thief entered into one of the email accounts that bore the username and hit password reset. But before they did this, they had done an illegal SIM swap on their cellphone to register it with the phone number of the executive's cellphone. Before the cell network deconflicted this error, the thief was able to receive the password reset text for the crypto-wallet application and input their own new password. Then the thief simply logged in and sent the funds to their own account.

Why It Is Inappropriate

This is more akin to traditional identity theft and fraud, and no code-execution, hack, or vulnerability was exploited from a cybersecurity perspective. Similar stories to this fictitious case study have been published on prominent cybersecurity forums and websites and across those and more traditional media are discussed as hacks and cybersecurity vulnerabilities, which only further permeates such misunderstanding.

Who Is Responsible

Theft like this is the responsibility of the victim, for publishing information that is used as their username, as well as data on what devices would be used to accomplish resetting the password. Perhaps, this could be

considered an issue with the cell network allowing SIM swapping to redirect traffic from one phone to the other. In neither case though, is this a cybersecurity issue.

Case Study 2

Crypto currency has exploded onto the scene in the past decade and for a while, new coins were being announced frequently and with no official, legal, or defensible verification process. What followed were events called initial coin offerings (ICOs) which pulled credibility from the similar initial public offering (IPO) for companies wishing to go public and generate funding. Essentially, the ICO was a company saying, if we get a certain amount of people to invest money into our crypto currency, we can launch it and be another successful, but probably smaller, version of Bitcoin, Ethereum, or others. This can also be done as a scam for malicious reasons too and result in ordinary theft.

What Happened

In this case study though, the thieves were pretending to stand up a new crypto currency and published and advertised their new ICO on a website they bought and paid for to appear as legitimate as possible. The scammers even registered a company with the same name and had a connivingly professional URL and technical jargon to convince would-be investors of the strength of the security in their crypto currency. With this scam infrastructure in place, they started their ICO event.

Once the ICO event concluded though, investors did not receive their crypto currency or accounts in crypto wallets listing their new digital assets. The thieves had simply gone through the effort of pretending to host an ICO and all of the investors had simply sent money to them and would receive nothing in turn. There is a twist though. The website the scammers registered put up a lone post, saying that during their ICO

they had been the victims of a hack and that they were terribly sorry for anyone's losses or inconveniences, but since they had also put all of their funds into the ICO as well, they were being forced to file for bankruptcy and liquidate the business.

In truth though, the scammers had not been hacked, they just used it as an excuse because it had happened to several other early ICOs. They said the attackers moved all the funds into some other account. But in this case, there was no actual hack or attack and the scammers had simply transferred the funds to another account themselves, using the fictitious hack as cover.

Why It Is Inappropriate

Once again, here there is no code vulnerability leveraged or exploitation that has happened. There is no hack that led to the compromise of the website and the victims have simply been duped into sending money just as in Case Study 1. There is nothing a cybersecurity professional should do here. While, in Case Study 1, it was media attention and cybersecurity forums that intonated it was a cybersecurity issue at hand, in this case study, it was the scammers themselves that sought to leverage the overextension of cybersecurity's boundaries for their own good.

Who Is Responsible

The obvious answer is the scammers are responsible for this since it was them who stole the money. But the individuals who bought into this scam bear some responsibility as well. These scammers knew they could prey on the eagerness of inexperienced investors to not do their due diligence and try and get rich quick. The difference in how this impacts the establishment of boundaries for cybersecurity compared to Case Study 1 is important. In the first example, the victims of email scams and the media are typically the ones crying foul against cybersecurity for not having prevented the email solicitation scam. In this case study, it was the thieves

that pushed the blame on to cybersecurity. Both are an impediment to the craft of cybersecurity, putting the body of work in an unflattering light via overextension of responsibility boundaries.

Case Study 3

In a militarily invaded country, a satellite Internet provider for the sake of altruism seeks to provide free Internet to the recently deprived citizens of that country, so they can continue to communicate despite the aggressor's attempts to destroy the IT infrastructure of the country. Unfortunately, electronic warfare (EW) emissions were being used by the aggressor to negate the capabilities of this newly delivered satellite Internet as well.

What Happened

The satellite Internet vendor publicly denounces the invader's attempt to jam and negate the vendor's ability to provide this vital service of Internet access to the citizens of the attacked country. In social media, the vendor's CEO even states that they have taken cybersecurity and other efforts necessary to protect their system from the effects of the enemy's EW jamming.

Why It Is Inappropriate

In truth, the fix to the issue was that a software update to the software-defined radio (SDR) components of the Internet service systems was able to get around the invader jamming certain frequencies by simply adjusting to new frequencies as was necessary. Neither the issue (jamming) nor the solution (updating programming) is a cybersecurity issue or solution. The implementation was done on digital devices (SDRs are essentially computers attached to antenna), but this is far outside the realm of cybersecurity.

Who Is Responsible

As stated, this was a programmed update to address the EW problem. Foresight on the part of the vendor could have enabled them to create programs that were capable of addressing degraded environments on their own. Even so, it was the vendor's electronic radio frequency specialists and programmers that fixed the issue, not cybersecurity professionals or solutions. So, why mention this case study at all? We have brought it up because while the first two case studies had the victim and then the thief being responsible for inappropriately roping in cybersecurity into the conversation, here we have a vendor themselves doing so. More careful messaging on social media as to the issue at hand and the fix and leaving out the term cybersecurity from that particular message would have prevented any potential interpretation of cybersecurity responsibility in this instance.

Responsibilities to Embrace

It is one thing to shirk responsibilities for cybersecurity where appropriate and sometimes necessary. As we have discussed, this is for the betterment of the industry as well as our consumers. It would be lazy to think that there are then no situations where cybersecurity as an industry or body of work could step in and provide further or previously unacknowledged benefit. These situations are likely to be more niche in nature and harder to come by, and admittedly, the issue at hand for this chapter is focused on the hampering nature of overextension. Still, if we are doing an introspective analysis, we should evaluate both sides of the argument.

Example: Be Your Own Enemy

The best example of something we believe could be considered a novel and beneficial approach to applying traditional cybersecurity roles and mentalities is an offensive assessment. In this book and others, the concept of offensive security are covered as truly proactive ways of securing an organization's attack surface by applying traditional (military) red team mentality to cybersecurity assessment in the form of services like penetration testing.

Our argument is that that mindset should be applied to other aspects of the risk equation. A penetration tester might look at an organization's computer or network and try to find ways of exploiting it or using it to exploit the organization. We argue for taking the mindset and applying it to things like cost-benefit and intelligence creation as well. Leveraging the attacker or red team mindset and assessing an organization provides insight into how cyber criminals might view that organization as a target. This can reveal the ways in which those adversaries may consider their own unique cost benefits when trying to compromise the organization. Further, this mindset could be applied to create cyber threat intelligence that could be used by the organization to help it secure itself through informing of hunt and detect activities. This sort of implementation allows an organization to focus not only on threat intelligence from known cyber threats and actors but to postulate their own, with their complete insider knowledge in ways that may prove uniquely insightful and help mitigate cyber risk in unconventional ways.

Learning to Leverage the Non-Cyber

There are non-cyber decisions that can be made by those not in cybersecurity that can impact the posture and attack surface of an organization more effectively that cybersecurity solutions. If it is important

to know what things to acknowledge cybersecurity should not be responsible for or things that should potentially be added, it is also important to know when cybersecurity is better served through un-security efforts.

What if there was a way to combine two things in one place without jeopardizing that which is most important? If the new normal is that everyone is going to be allowed to have access to all their personal accounts at work, then how do organizations and their cybersecurity professionals make sure their policies are implemented and enforced to protect their data while allowing employees their ability to use personal accounts? what if there was a way to allow this without the accounts of the employees having to ever touch the organization's network or having access to the organization's data?

Could a simple separation of two networks be the solution? The organization could have their network that would be restricted to only the applications and data that are truly needed for the employees to perform their jobs and the mission of the organization. Another network could be stood up and accessible to all employees but would be open and more of a use-at-your-own-risk, with minimal resources being spent monitoring or defending it. The restricted network would be the cybersecurity professional's sole responsibility to defend and operate as it will contain all the organization's data. While the open network will allow for employees to use for personal applications such as social media and checking personal email accounts, it will not contain any data from the organization. While there is an added cost for providing the open network with separate hardware and another service contract with an Internet provider, there is a reduction in risk and less man-hours spent trying to monitor and defend the organization's network from every employee's personal accounts. This would be a low-cost solution that reduces risk to the organization while providing Internet access for employees to use for personal applications.

Example 1

Assume you are the CISO of a company that makes sneakers. You are reviewing your organization's cybersecurity resources, such as staff and software licensing, because there is a cut to funding and the ask from the organization has been to find something to cut. Log and traffic monitoring is one of the highest cost expenditures your organization has from both a staffing and a licensing standpoint. The licensing for the software used to collect, aggregate, and analyze logged events and network traffic flow within the organization charges on a traffic-volume basis. Further, because of the amount of traffic being collected, analysis and response to incidents by cybersecurity staff make up a bulk of the hours allotted from a salary standpoint in the cybersecurity department.

After a quick look through these resources, you find it difficult to cut other cybersecurity personnel or software requirements, so you return to the log and traffic collection issue. You notice that almost 25% of the traffic collected, aggregated, and analyzed for malicious activity are entirely from social media websites and platforms that are in no way involved in the operation of the organization or the execution of tasks toward accomplishing strategic goals. If this sort of network traffic was simply denied, from both a policy and filtering standpoint, there would be an extra 10% personnel hours and software budget overall for the cybersecurity department which would meet the necessity of the proposed budget cuts and would not detract from the security posture of the organization or the defense of its cyberattack surface.

This means you can reduce the budget, which aids the organization in accomplishing its strategic goals. Further, the organization's risk exposure is also lowered as common mediums for various attacks and exfiltration of sensitive information have been removed from the network. This was accomplished without any need for further cybersecurity implementations or solutions and should be an example of a first step that could be taken by an organization to address its cyber risk and not a last-ditch defensive

effort by the cybersecurity department to avoid budget cuts. It is again an oversimplification of a situation within an organization, but it illustrates the importance of understanding where the boundaries of cybersecurity roles and responsibilities lie and how non-cybersecurity efforts can make them easier to maintain.

Example 2

Let's continue with the same role and company as Example 1. You are the CISO and the business model is to sell sneakers, as many as possible for as long as possible. That would be the business strategy of the organization. The CEO has tasked you with using some of your cybersecurity budget to ensure the organization can withstand the impacts of cyber compromise and continue operations.

You begin researching implementations for servers and user machines to be more resilient to individual cyber compromises so that they don't end up having larger, more widespread impacts on the business. You find that such virtualized solutions come with their own cost models, and they are in some places cheaper, and in others, much more expensive than your current architecture. In all cases, however, because you do not currently operate in the cloud or a virtualized environment, they are a new cost. Further, going with said solutions can result in a sort of waste of already sunk costs in physical infrastructure you already operate from as they would fall into obsolescence.

Worse still, you do not have in-house cybersecurity expertise to correctly leverage these technologies and platforms, which means even more money would have to be spent on training or hiring. You know the CEO's goal is resilience to cyber compromise and to avoid that as a risk to the business strategy. What if you challenged the rest of the organization to help mitigate such risks from non-cyber perspectives? What sets your sneaker company apart from others is that you allow custom orders of sneakers, and they are then processed and made to order and sent out.

The same chain of devices that handles orders also carries credit card information from the purchaser to the company's accounting department. This means that risk to company operations and risk to customer data ride along the same paths and that compromise of any device along this chain of devices can impact both revenue and reputation.

You ask if it would be possible to have the order placed on the website send that data directly to the shoe manufacturing devices and those devices would then send an appropriate invoice to the accounting department. This would allow the accounting devices to then send an invoice to the purchaser, ensuring that financial data only passed from customer to accounting and that shoe creation data only passed from customer to manufacturing devices. This separates the revenue and potential reputation risks into segmented parts of the organization and would make both sides more resilient to a ransomware attack in one or the other. This allows for non-cyber decision makers to weigh in on a situation that can simplify the architecture the cybersecurity staff have to protect without turning it into a tax on the organization's operations.

This sort of example can also exist in a completely non-cyber state where doing something as simple as spending the money to create a three-month stockpile of certain ingredients for sneakers would make you resilient to threats such as ransomware on your logistics and ordering servers. If the three-month supply of sneaker ingredients and storage of them is cheaper than the cybersecurity solution to make the logistics servers resilient, it would probably be better to go with the non-cyber option. This is especially the case because an on-hand supply increase like that is something that will always eventually be utilized and will be seen by someone such as a CEO as less of a dead cost or paid tax than cybersecurity might.

Building the Right Size Box

Typically, we security professionals are preaching outside the box thinking, but perhaps, as illustrated by previous examples that has maybe gotten us overextended. The motivation may have been to broaden consumer's exposure to cybersecurity, but that lens is probably too wide. These decisions should be tailored and right sized to fit the organization's strategic goals and be appropriate to the resources available to that organization or otherwise inform the accumulation of those necessary resources.

Everything is now connected, and everyone has multiple devices that they carry with them everywhere they go. There are smart watches, smart phones, and even smart glasses; everything is becoming smart and, in doing so, allowing constant access to the Internet. It's this constant connection that must be evaluated to determine what risks we are willing to accept and why.

To understand where to draw the line or what is to be allowed in the cybersecurity box, there must be a true understanding of what devices are critical from a cyber perspective for a company to complete its intended purpose. This one piece of knowledge can help to stop the mission creep for cybersecurity professionals inside the company. When trying to apply cybersecurity without the internal knowledge of what truly needs to be protected, the security can become thin and/or overstretched trying to protect everything. Focusing on protecting from the inside out allows you to identify where areas can be included rather than a blanket security policy. The one size fits all for cybersecurity practice is both human and computer resource-ineffective.

Allocating cyber resources to critical areas and reducing or eliminating them in areas that are not directly related to productivity or are simply a nicety for the employee allows for a more focused implementation of resources. With this information, you now know the bare minimum that must be supported and protected. This may, when really looked at, be a server in a closet with only a few truly needed connections to it.

There needs to be a self-assessment of what a likely attack on your organization would actually be and what would be the targeted area inside the network. In the news, there are countless reports of ransomware being deployed against local governments, the natural gas industry, and other organizations. These organizations all provide products or services that, if they were unavailable, would cause a considerable disruption. There is also a presumption that, if ransomware was deployed, there is an ability to pay the requested ransom. What does your organization provide? Should there be reason for concern of a ransomware attack? Would the value of your data be more valuable than the service you provide? Then there is the fear of data exfiltration that must be considered.

Understanding what your organizations value as a target will focus resources and help identify potential attack types. As a small company, the likelihood of being targeted with ransomware is probably lower since there is less perceived money for the attacker to receive. Conversely, if your organization has data of high value of individuals or other organizations, then that information may be seen as more valuable and therefore a targeted resource. There is always the chance of random attacks against the organization. So, what does building an appropriately sized box for a specific organization's cybersecurity look like?

Step 1: Know Thy Cyber-Self

In Chapter 2, we discussed how the taxonomy of where roles and responsibilities fall within the expansive and diverse body of work that is cybersecurity. To protect any organization with cybersecurity services or products, that organization must clearly understand what the roles and responsibilities are of what resources it already has in place. This requires a more in-depth understanding of the taxonomy of cyber roles that is typically expected or presumed. Without this knowledge though, an appropriate definition of what is and is not the responsibility of those people, services, and products cannot be accomplished.

Step 2: Prevent What Is Known

Before you do anything else or can hope to achieve strategic or theoretical gains in cybersecurity application, the known threats must be prevented first or there is no cost benefit in expanded approaches. The aim of this book is to suggest that the envelope must be expanded or pushed in new directions. However, it would be folly to not accept that there are minimum, non-theoretical efforts that must be in place before innovation and improvement can be pursued. Known threats and existing vulnerabilities are things that must be focused on first and foremost. To spend time on theoretical or novel cybersecurity applications in the hopes of better addressing risk within the constraints of cost benefit before doing so is foolhardy.

If available cybersecurity resources cannot prevent or mitigate what is known and already observed as cyber threats and risks, there is no sense leveraging them in other ways. This statement is not meant to stymie efforts at improving the body of work that is cybersecurity. It is to ensure that innovation takes place responsibly, after what should be commonly implemented countermeasures and protections are already in place. To do otherwise risks unsophisticated compromise that endangers cybersecurity consumers and the reputation of cybersecurity producers.

Step 3: Know Thy Strategic Self

Beyond knowing what cybersecurity assets are at the disposal of an organization, it is also imperative that the organization and its cybersecurity staff understand the long-term goals and tasks (cyber and non-cyber) that are integral to the organization. Without this knowledge, it is impossible to establish cost benefit in general or as it specifically relates to resource expenditure on cybersecurity to protect said goals and tasks from risks to its attack surface. Without knowledge of cost benefit and risks in this sense, the cyber box may have boundary lines based on available abilities, but what they are placed around is yet unknown.

Step 4: Leverage Non-Cyber

As was shown in several examples earlier in this chapter, risks to an organization are not always best addressed through cybersecurity implementations. Further, cybersecurity issues and risks can at times be more efficiently mitigated through non-cybersecurity choices and implementations. The potential for these sorts of solutions should be assessed and exhausted before cybersecurity is fully leaned on to solve various problems. This means that security staff need to be empowered to prevent the baseline, known, preventable threats and then be brought into conversations regarding an organization's strategic tasks and goals, so they can participate in the enabling of said goals and tasks and whether cybersecurity is the best or most cost-beneficial solution available.

Most consumers of cybersecurity are not cybersecurity producers. It should therefore go without saying that leaning on an organization's organic and native expertise to address risks first, cyber or otherwise, will lead to the most efficient solutions to such problems.

Step 5: Calibrate and Implement

At this point, we have identified our organization's cybersecurity resources and their roles and responsibilities. We have enabled them to prevent the bare-minimum acceptable number of cyber risks based on known threats. We have informed the cybersecurity apparatus on what the strategic goals and risks of the organization are, and the organization has worked together with its cybersecurity staff to burn down additional risks with non-cyber solutions where able and appropriate. Next, we should look to adjust roles and responsibilities that are carried out on our cybersecurity resources to focus on what is most necessary to achieve good cost benefit, while only expecting cybersecurity personnel, services, and products to function within established boundaries of responsibility. At this point, it may be necessary to expand or contract in certain functional areas of

the cybersecurity taxonomy to achieve the most cost-beneficial results necessary, only after exhausting internal non-cyber solutions as well. Aside from leveraging tribal knowledge and organizational expertise, such solutions have the benefit of being viewed as less of a sunk cost or tax, as the operational staff of the organization more readily understand the cost benefit of such implementations that reduce risk. Whereas, in cyber this may be harder to communicate.

Step 6: Reassessment

It is not enough to identify and calibrate an organization's cybersecurity response to strategic risks once. Any successful enterprise, commercial or otherwise, relies on adaptability to environments and events as well as the passage of time to stay relevant and operational and maintain strategic continuity. Any periodic re-evaluation that supports these goals and tasks must also include cyclical recalibration of the cybersecurity apparatus that supports the risk mitigation of that organization. Figure 4-1 illustrates this process.

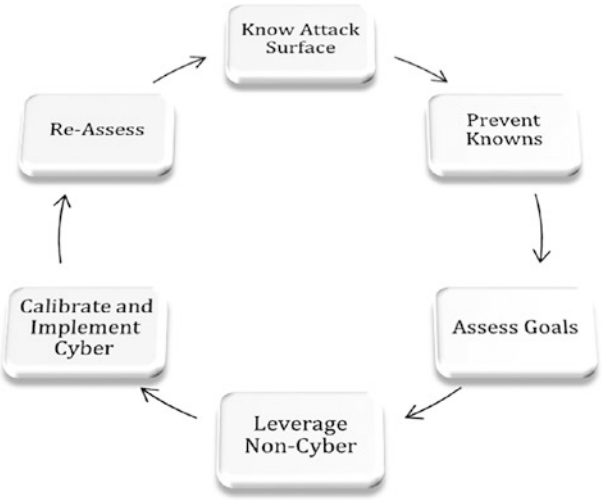

Figure 4-1. *Building the right sized cybersecurity box*

Summary

We have discussed in this chapter that one of the bigger challenges to successful cybersecurity and cybersecurity innovation and theorization is poorly defined boundaries. Our ability to define what roles and responsibilities fall within and on the periphery of our body of work is integral to having a strong foundation from which innovation can build upon. The case studies presented, and the process proposed are just our examples on ways to understand how organizationally specific boundaries can be established. This will allow us to address cybersecurity risk appropriately with resources that are not overextended. We will learn how to communicate with the wider organization in ways that present cybersecurity risks as addressable through non-cyber means. Further, through cyclical establishment, analysis, and defense of appropriate roles and responsibilities we can better position theoretical cybersecurity innovation on both a by-organization and body of work basis.