WHITE PAPER

Building a Culture of Cybersecurity

A Guide for Corporate Executives and Board Members

APRIL 2018

CompTIA

Table of Contents

Cybersecurity is an executive-level issue

Warren Buffet recently cited cybersecurity as the number one issue facing humanity—more dangerous even than nuclear weapons. If one of the world's preeminent investors, who quantifies business risk and opportunity every day, is paying so much attention to the issue, every executive and board member should, too. And many are. According to the World Economic Forum, a majority of business leaders indicated that cyber-attacks are their top concern heading into 2018.[1] Much of this attention is likely driven by the substantial—and costly—growth of cybercrime. It is estimated that in just three short years, cybercrime damages will reach $6 trillion annually, making cyber-attacks more profitable than the trade in all illegal drugs, combined.[2]

The rapidly changing business environment is also exposing companies to more cyber risks. The explosion of interconnected devices, adversaries' hunger for "big data" analytics, and the outsourcing of critical business functions are just some of the forces that are making companies more vulnerable to attack. Company leaders are tasked with striking a difficult balance between keeping up with their competition and defending against escalating threats.

In addition, regulatory scrutiny is intensifying around the globe. Most notably, in the European Union, the General Data Protection Regulation (GDPR) promises hefty fines for companies that fail to adequately protect consumer data. In early 2018, the U.S. Security and Exchange Commission (SEC) released new guidance that demanded more extensive cybersecurity disclosures and called on boards of directors specifically to incorporate cybersecurity strategies into their broader risk management processes.

> "In a McKinsey survey of corporate directors, …almost half claimed that the attention they gave to technology was insufficient. More than half of board members also felt they should hold more discussions about how technology will affect their industries…."

As a result of these forces, many in senior management feel the increasing need to address cybersecurity more effectively. More than one-third of directors in North America, Australia, and Western Europe claim that cybersecurity is a top issue for their business.[3] Yet, even those who recognize the importance of cybersecurity may not feel confident they are taking the right steps. In a McKinsey survey of corporate directors, the majority of respondents reported that their boards had at most one technology-related discussion a year, and almost half claimed that the attention they gave to technology was insufficient. More than half of board members also felt they should hold more discussions of how technology will affect their industries in the coming years, but fewer than 30% actually had these kinds of discussions.[4] Only one-quarter of boards

report that they review formal reports from the CIO at every meeting, and on average boards claim to spend about 5% of their total hours each year on IT oversight.[5]

Thus, there is a gap between how important cybersecurity issues are and the amount of involvement in those issues by senior company leaders. This disjuncture is a direct result of the "knowledge gap" between most executives and cybersecurity professionals. Corporate leaders typically have considerable managerial experience and business acumen, rather than narrow, technical expertise. Most do not have the requisite knowledge to properly analyze the technical information given by cybersecurity professionals. Similarly, cybersecurity professionals often lack knowledge about risk management, corporate governance, and strategic planning, which makes it difficult for them to communicate effectively with senior leaders. Thus, the "knowledge gap" can also quickly become a "communications gap," too.

However, to manage a complex challenge like cybersecurity, an organization must be able to collaborate across disparate functional areas—including defense, prevention, detection, remediation, and incident response. Such coordination requires that company leaders openly share their expertise, agree upon priorities, and ensure that security efforts are aligned with business objectives.

Senior leaders are uniquely situated to lead the kind of coordinated response that cybersecurity requires. Because they sit at the top of the organization, they can see across departments, which gives them a more comprehensive view than business unit managers have. They are also bestowed with the authority to ensure that groups work together—even those that do not always see eye-to-eye or share the same objectives.

Because corporate leadership is also responsible for managing risk across the organization, executives and board members must ensure that cyber risk is managed using the same framework as all other risks the company addresses. Failure to take leadership on these issues can have disastrous consequences in the event of a breach, including high profile job losses, protracted lawsuits, and heightened regulatory expectations.

In short, cybersecurity strategy must be established and managed at the highest levels of the company. To do so, however, will require a shift in mindset for many organizations. Security can no longer be isolated as a technical problem with a technical solution; it must be prioritized as a critical business concern. In fact, the greatest weakness in most companies' security is not their technology, but their people and processes. Only about 3% of the malware that Symantec handles seeks to exploit a technical flaw. The remaining 97% of attacks attempt to trick a user to unwittingly hand over valuable data or information.[6] Defending against these kinds of attacks requires more than just the latest patch or upgrade. Instead, the company culture must emphasize and value cybersecurity. Senior executives should—and must—lead this change by providing adequate resources and using cybersecurity metrics as key performance indicators at their companies.

This paper arms senior executives and board directors with the necessary knowledge to guide their organizations' cybersecurity strategy and execution. It focuses on how to create a culture that values cybersecurity, and it provides principles, or guidelines, to help company leaders drive progress in their organizations by coordinating company teams and resources, rather than continuing to silo cybersecurity as primarily an IT concern.

Using this white paper to guide your actions

This white paper begins with an overview of cybersecurity threats, issues, and considerations, especially in terms of the business concerns most important to boards and company executives. It then articulates and explains six guiding principles that will enable senior leaders to assess and improve their organization's approach to cybersecurity. These principles are:

1. **Integrate cybersecurity into your business strategy.**
2. **Your corporate structure should reinforce a culture of cybersecurity.**
3. **Your employees are your biggest risks.**
4. **Detect, detect, detect.**
5. **Data protection: collect what you need, share only what you have to.**
6. **Develop robust contingency plans (and test them!).**

The discussion of each principle includes a detailed explanation of the most pressing concerns that executives need to consider, an overview of potential threats and opportunities, and a set of tools and checklists to help follow through on that particular principle.

We opted for a discussion of principles in order to make our positions clear and actionable. The paper is informed by concepts outlined in the Framework for Improving Critical Infrastructure Cybersecurity released by the National Institute of Standards and Technology (NIST), which provides a comprehensive view of how to build a solid cybersecurity foundation through a series of steps—Identify, Protect, Detect, Respond, and Recover. This paper builds on NIST's framework, as well as other organizations', to offer a set of guiding beliefs, listed in order from the most fundamental to the most business-specific.

These principles are intended to guide you in creating evaluative matrices so that you can take immediate action to meaningfully improve your organization's cybersecurity readiness. Documents like the NIST framework offer important tools for building an entire cybersecurity apparatus. This paper will empower you to better assess the structure you have in place, helping you focus and prioritize your efforts. We encourage you to view these principles through the lens of your particular organization. Customization is critical because effective security is not a "checkbox" type of activity.

Emerging threats in cybersecurity

When examining recent high-profile attacks, one theme becomes clear: many of these notable breaches occurred at "compliant" companies, including Target and Equifax. The takeaway is that simply meeting legal requirements is not enough to prevent cyberattacks. To create a culture that values cybersecurity, management must think beyond what is legally required. Cybercriminals aren't worried about your organization's cybersecurity requirements or standards. They simply want to find and exploit the weak points in your system.

As technology advances, attackers need less technical knowledge and fewer resources, while defenders need substantially more capabilities and multi-layered systems. State-sponsored groups are using ever-more sophisticated methods, and evidence suggests that gangs of cybercriminals are now selling their services to the highest bidder. As these dangerous individuals band together, defense still falls largely on individual companies.

In addition, the increase in the number of interconnected devices provides crimin
als with more targets to exploit, and breaches are becoming both more severe and more frequent.

To effectively lead cybersecurity efforts, it is imperative that executives understand the most prevalent kinds of attacks and how they operate. The most notable attacks include:

Ransomware: Ransomware continues to be one of the most dominant threats facing organizations. In a ransomware attack, an organization's hardware, software, or data is held "hostage," and criminals demand payment to unlock it. These attacks are typically delivered via phishing emails that target individual employees, who are usually instructed to click a link in order to pay the ransom. Often, the link itself is corrupted, so even if the employee does not pay the ransom, the system can still become further infected.

Lessons Learned from High Profile Breaches

Target	In 2013, cyberattackers breached Target's computer systems via a third-party vendor. The attackers the gained access to the retailer's customer service database and installed malware that captured personal information on some 60 million consumers. A $10 million class-action lawsuit was settled in 2015, and in May 2017, it was announced that Target would pay an additional 18.5 million in a multistate settlement—the largest amount ever for a data breach. Yet, Target has generally been lauded for its equally far-reaching and effective response. Not only has it avoided similar attacks, it has created a customized security framework, which uses powerful analytics to protect its most sensitive systems.
Dyn	Dyn is a domain name system (DNS) provider—a service essentially connects a web address, which users type into their browsers, to a specific IP address. In 2016, the company suffered multiple distributed denial-of-service (DDoS) attacks which completely shut down major web sites in the U.S. and Europe, including Netflix, Amazon, and Spotify. The Dyn attack was likely caused by a botnet, coordinated through internet-connected devices that were infected with malware. This high-profile event showed that DDoS attacks remain a serious issue and that companies must create resilient networks in preparation in case of attack.
Equifax	Personal information—including Social Security numbers, birth dates, and driver's license numbers—of 145.5 million consumers was compromised in a data breach that dated back to March 2017, though the company did not report it for six months. In the wake of the poor handling of the breach, CEO Richard Smith stepped down, as did the company's Chief Information Officer and Chief Security Officer. In February 2018, Equifax revealed that even more data was stolen than initially claimed. Equifax's handling of that breach—from its irresponsible handling of data to its inaccurate public statements—has been roundly criticized. Not only did the company fail to address the known vulnerabilities, senior leadership was poorly informed, slow to respond, and deliberately misleading.
Uber	It took Uber almost a year to admit that 57 million users' personal information was stolen in a ransomware attack. Rather than disclosing the incident, the company paid $100,000 in ransom to have the stolen information deleted. Follow-up investigations found that the hacker broke into Uber's Github account, a third-party, cloud-based service that many companies use. Following the announcement of the breach, multiple states' attorneys general launched separate investigations, and the company has also had to answer to the Federal Trade Commission. Subsequent reviews revealed a persistent disconnect between cybersecurity professionals and senior management when it came to understanding, measuring, and prioritizing important cybersecurity metrics. The case underscores how vital it is for business leaders and technical professionals to collaborate and align their goals and values.

More than 4,000 ransomware attacks occurred each day in 2016 alone—a 300% increase over 2015.[7] Cybersecurity Ventures reports that ransomware damage costs exceeded $5 billion in 2017, up more than 15 times from 2015.[8] Yet studies show that only 47% of victims who pay the ransom ever recover any files.[9]

Ransomware-as-a-service (RaaS) attacks are also on the rise. In this variant, criminals do not even need to write their own code. Instead, they simply log onto a site, configure their particular attack, and distribute the already-written malware to their victims. Such technology makes it even easier for aspiring criminals to launch large-scale attacks.
Ransomware also adapts quickly to new defenses and technologies, and new variants evolve quickly. Some attacks, including Troldesh and GlobeImposter, now target the Graphics Processing Unit (GPU), instead of the CPU, enabling the malware to spread hundreds of times faster. Other strands now include multi-level marketing attacks, such as Popcorn Time, which force victims to choose between paying a ransom directly or infecting additional victims themselves.

Internet of Things: The Internet of Things (IoT) is a network of physical devices, embedded with electronics, software, and sensors that enable these objects to connect and exchange data. Although many companies are excited by the potential, these devices also pose a significant security weakness. This is because they are often activated with their default passwords unchanged and are thus easily compromised.

Once criminals break into these devices, they can use them to create botnets, which can unleash large-scale attacks to steal data, to identify further vulnerabilities, or to mount brute force attacks, like the DDoS attack on Dyn.

McAfee Labs identified the rise of artificial intelligence as one of its top five threat predictions for 2018, describing an "arms race" between attackers and defenders, in which both sides hope to maximize the power of machine learning.[10] Attackers are using AI to improve social engineering attacks and make them even more difficult to recognize. Defenders are using AI for automated breach prevention—an evolution from using it for detection only. Attackers, however, appear committed to learning as much about these new defense systems as possible, and machine learning can help them scan for vulnerabilities much more quickly, which in turn means that detection systems must be all the more nimble and prepared.

No one can predict what new variants will emerge or when, but it is clear that cybercriminals are determined, creative, and emboldened. To protect against the increasing threats, your cybersecurity strategy must be well coordinated, appropriately prioritized, and responsive, and it must extend across your organization. This paper and its principles are intended to help you create such a culture.

Principle One:
Integrate cybersecurity into your business strategy

Each year, the Ponemon Institute administers a global survey to determine the cost of data breaches around the world, quantifying various factors including: lost clients (churn), the number of compromised records, the time it takes to identify a breach, and the post-breach costs, such as notifying affected customers.[11] To determine how much a breach might cost your particular organization, there are many tools and calculators that can help you quantify relevant expenses.[12]

Executives often approach cybersecurity with the mindset of the "defender's dilemma"; they worry about the damage that one data breach could cause. But it is difficult to quantify the benefit of avoiding an attack. How can cybersecurity professionals demonstrate their worth when their success is determined only when something doesn't happen?

No highly trained professional wants to constantly prove their value, and in a competitive employment landscape like cybersecurity, your organization probably shouldn't send the message that such continuous justification is required.

The first principle of this paper, therefore, is that company leaders must measure the value of cybersecurity more accurately and do so from a broader business perspective. Think in terms of the processes your organization can put in place to create better response times and to manage containment failures more effectively. This kind of focus takes the onus off of the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to do the impossible: prevent all attacks or risk the appearance that they have failed. Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business and lead the way in advancing new approaches to cybersecurity costs—and returns.

"Senior executives and board members need to be directly involved with quantifying cybersecurity efforts across the business and lead the way in advancing new approaches to cybersecurity costs—and returns."

Think of cybersecurity as an ROI proposition

Without question, companies are spending considerable resources on cybersecurity. As just a few examples, in 2017, J.P. Morgan Chase doubled its annual cybersecurity budget to half a billion dollars, and Microsoft said that it plans to invest more than $1 billion annually on

cybersecurity research and development in the coming years. In total, Cybersecurity Ventures predicts that global spending on cybersecurity products and services will exceed $1 trillion cumulatively by 2021.[13]

However, simply increasing spending on cybersecurity won't improve your company's results. Senior leadership must make sure that this spending is directed properly. Because budgets are limited, priorities need to be weighed and established. Yet, research shows that executives tend to distribute resources evenly among threats and testing methods, rather than focusing their efforts.

Because cybersecurity issues affect so many other threats a company faces, including operational, financial, and legal risks, the board should view cybersecurity as part of its larger responsibility to manage organizational risk. Cybersecurity should be assessed in the context of a company's strategic plan, in which risks are balanced alongside growth opportunities. To do so requires collaboration between senior leadership and cybersecurity professionals, who can best determine the proper risk management steps.

Applying a risk-rewards analysis to cyber threats can be intimidating for senior leaders, especially since breaches can generate embarrassing headlines—and even worse, class action lawsuits against directors and executives. As a result, it can be difficult to keep fear from overtaking your cybersecurity policy. After all, no one wants to be associated with taking a risk if an incident later occurs.

Directors' fears about litigation are understandable, but it is important to note that many court cases have focused on whether the board had adequate cybersecurity policies and procedures in place, especially in writing.[14] In most cases, courts and regulators have focused on whether directors have taken their cybersecurity obligations seriously and have not attempted to evaluate directors' specific business decisions. What matters is whether the boards appropriately discussed cybersecurity threats and remediation, not that they created perfect plans that could prevent every possible encroachment.[15] This is not to suggest that boards can be cavalier when making strategic decisions, but it serves as a reminder that legal precedence emphasizes the need for an established cybersecurity risk management process. Understanding this might help reassure board members when making risk-reward decisions about cybersecurity.

When considering ROI, it is also important for executives to understand that many basic cybersecurity tests cost very little to execute but can provide valuable returns. For example, regular "phishing tests" are relatively inexpensive but can substantially increase security awareness. In these simulations, individual employees receive e-mails that prompt them to engage in risky behaviors, like clicking an unverified link. Individuals who are tricked by these fake e-mails are then informed that this wasn't a real attack and are taught how to avoid similar traps in the future. Often, very inexpensive tests like these can significantly decrease the likelihood of a very costly attack.[16] Viewing cybersecurity from this cost-benefits perspective can make your efforts more efficient and effective.

Similarly, the technology required to protect most systems is often not as sophisticated or costly as many senior leaders might assume. However, the implementation of this technology does need to be considered and prioritized. For example, imagine a company that creates a new policy that requires two-factor authentication, but some of the organization's legacy servers cannot be easily—or inexpensively—upgraded. If the rest of the network can compensate for these servers and significantly lower the company's overall vulnerability, it may be more prudent to accept the small risk of the non-compliance of a few servers rather than devoting resources to upgrading them. It may also be prudent to consider purchasing cyber insurance to transfer the risks posed by these servers. Given limited resources, it is best to focus on protecting against the more serious or more likely threats, and company leaders are the ones best positioned to make these sensible, justifiable risk decisions. Such judgments, however, require that senior executives and cybersecurity professionals engage in regular, productive conversations about ongoing threats and possible solutions.

Identify your company's data "crown jewels"

A robust cybersecurity strategy must identify and prioritize the data, systems, and other assets that are most important to the company's competitive position—what are often referred to as a company's "crown jewels." Only after identifying these critical assets can a company determine whether it is spending wisely on cybersecurity resources.

Your data "crown jewels" are unique to your company. They are necessary for your company's brand identity, business growth, and competitive advantage. As such, they are often quite sensitive. They could include trade secrets, product design, or customer behavior data. When setting company priorities, management should place the greatest emphasis on protecting these "crown jewels," rather than applying a one-size-fits-all security solution across the organization.

See the Appendix for a step-by-step guide to identifying your company's data crown jewels.

Make sure that your senior team agrees upon what these "crown jewels" are; that they are truly mission-critical; and that they generate a competitive edge for your business.
Once you've identified your "crown jewels," then you can more clearly focus on how to protect them. Many companies decide, for example, not to store their most sensitive and important data in the public cloud. This may increase the costs to maintain, store, and protect this data, especially as it accumulates over time. But those costs are often outweighed by greater security and control over the data. A company may also decide that other information it collects is not as sensitive or valuable (to itself or outsiders) and might choose to store that data on a cloud application in order to conserve resources.

Where to store the "crown jewels" is just one issue to consider. You should also discuss what additional protection and detection measures may be appropriate. Of course, these measures will depend on your organization and the "crown jewels" it protects. You should also work with your security team to develop a threat matrix specifically for this data, which should be regularly updated.

Company management should integrate cyber-resilience into broader business strategies

In addition to securing the valuable data you already maintain, evaluating cybersecurity risks should be an essential step when considering new products, services, or operations. When assessing opportunities, board members and executives must lead the discussion about identifying cybersecurity risks and ultimately decide whether those risks are worth taking on.

These discussions will involve different elements of the organization as they progress. Business unit leaders are often the best situated to recognize and quantify the potential benefits of a new venture, and the potential to boost the company's bottom line can be very motivating and persuasive. On the other hand, cybersecurity professionals typically can best identify the inherent risks that accompany these opportunities.

Directors and senior executives should integrate cybersecurity risks into the tools they already use to evaluate new opportunities, such as:

- Scenario modeling
- ROI analysis
- Competitive analysis
- A formal review of emerging technologies

Rather than pit these two groups against one another and let them fight for control, a strong leadership team will facilitate, guide, and ultimately decide on the appropriate course of action. This means that the executive team must understand accompanying security risks and strive to realistically evaluate the new business opportunity.

This does not mean that new business opportunities should be rejected because they involve cybersecurity risks. All business initiatives always involve some forms of risk. Companies can also look to adopt principles, such as security-by-design, in order to intentionally build security into any new products or services.

Some risk-rewards of increasingly popular technologies include:

Mobile computing – Mobile devices are often more affordable and can be very beneficial in industries with extensive field personnel. A robust mobile policy is necessary, including how employees can use their devices for personal purposes or how to safeguard your data if employees bring their own devices. This practice is referred to as Bring Your Own Device (BYOD), and while many security professionals denounce the practice, it is becoming increasingly popular. Be aware of "the vanishing perimeter," which refers to your network being less defensible because employees are using devices and connections that are not under your purview.

Cloud services – Cloud services use the internet to access computing power, and they can increase efficiency and lower cost. With these advantages also come cybersecurity risks. The "cloud" provides a good example of why cybersecurity is about balancing risk with reward. Cloud computing is almost a necessity in many industries, and rather than trying to do business without it, companies should instead assess the risks and determine how to mitigate them. One possibility is to consider implementing a private cloud, which is housed on company servers, so it is more controlled, though it typically does not offer the same flexibility or scale as a shared, public cloud system can.

Some executives still perceive the cloud as inherently insecure. They may have heard about cases where migrating data to the cloud resulted in security issues. In many of these instances, however, the problem was not the result of "the cloud." Instead, a risk came to the surface when the company attempted to transfer its poorly-secured systems to the cloud, and that transfer revealed how weak the system was in the first place.

Software-as-a Service (SaaS) – With SaaS technologies, a company does not need to license, house, or maintain software because it is housed, along with the associated data, on a third-party server, accessed via a web browser. Business unit leaders are often eager to adopt SaaS applications, which are readily available and easy to use, and they do not require the assistance of the IT department—a group that can be perceived as raising objections or causing delays. Many administrative applications, like accounting and human resources, are now handled through SaaS applications. Such programs provide efficiency and scalability at relatively low costs, but they also increase risk—risk that company management may not even know about if the applications haven't been officially approved. It is important to develop a policy to cover SaaS applications, which delineates decision-making processes, necessary steps for approval and implementation, and the values that justify the move to web-based software.

Big data – Companies are increasingly interested in analyzing large sets of data to establish competitive advantage. Directors and executives need to evaluate the value of all this data, weighing that against the risks of collecting and storing so much information. In addition, it is often resource-intensive to mine the data for valuable insights. If the data won't be used and analyzed well, is it worth keeping? Will the insights be worth the risks?

Outsourcing – Third-party vendors and consultants can help generate efficiencies and cost savings. But with them always comes increased risk, especially (but not exclusively) when it comes to outsourcing IT services. However, it may be impractical, especially for small businesses, to handle all services in house, so company executives must determine what services are worth the risks that come along with outsourcing. You should make sure that your company carefully audits and evaluates each potential vendor. It's often the case that criminals will try to exploit relationships between third-party vendors and their clients.

Thinking this way requires a corporate culture shift, not new technology

Cybersecurity is a people, process, and business issue. It is not merely a technical issue. Within the NIST Framework, the organizations deemed the most "sophisticated" and "rigorous" are those that approach cybersecurity as a cultural, rather than technological, concern. For such organizations, NIST explains, "Cybersecurity risk management is part of the organizational culture."[17] The point is that risk management can't simply be an afterthought or an add-on. Security must be a core principle.

"...risk management can't simply be an afterthought or an add-on. Security must be a core principle."

It is important to remember that compliance is not the same as security. Compliance is necessary, but true security needs to go much further. This is why some experts prefer the term "cyber resilience" to "cybersecurity." It reinforces the assertion that cyber strategies should not merely be defensive but should position the company in a forward-thinking way. And as the World Economic Forum has concluded, "...cyber resilience is more a matter of strategy and culture than of tactics."[18]

The NIST framework can help executives consider cybersecurity in terms of business goals, rather than just as technological specifications. NIST even offers a nine-page outline to help board members create a step-by-step path to more robust cybersecurity.[19]

Cultural shifts like this can take time, particularly in organizations where cybersecurity efforts are historically underfunded or new altogether. Adopting a long-term view and remaining consistent are the keys to success in these cases.

Principle Two:
Your corporate structure should reinforce a culture of cybersecurity

A cultural shift to embrace cybersecurity should not just involve mission statements and articulations of company values. The structure of your organization—including reporting lines and compensation packages—must also reflect the importance of cybersecurity. If you do not explicitly build cybersecurity into your organization, you communicate that you are not truly committed to the goal.

Boards should appoint one member to specialize in and report on cybersecurity issues

Board members are increasingly recognizing the importance of integrating technical expertise into their decision making. In 2016, 45% of boards engaged an outside consultant to advise them on IT issues during the year, up from 27% in 2012.[20] As many as 37% of directors reported that they believe it is very important to have directors with IT strategy experience on the board, and 25% of directors "very much" believe that their company's IT strategy and risk mitigation approach are supported by sufficient understanding of IT at the board level.[21]

Thus, we recommend—along with other experts and government organizations—that at least one member of the board should have expert-level knowledge of cybersecurity issues, so as to help close the knowledge gap between cybersecurity professionals and board members.[22] This person should be accountable for reporting to the board about the company's preparedness for dealing with cybersecurity threats and implementing preventative measures. The entire board should still remain involved in and informed about cybersecurity issues, but at least one member should have the technical background to help translate pressing issues in business terms. This helps avoid putting cybersecurity into a "silo," managed primarily by IT departments. Such positioning is especially important since cybercriminals are particularly adept at exploiting siloed systems and communications.

Other structural issues that board members should address include:

- Should the whole board actively monitor cybersecurity threats, or is it better to have it overseen by a dedicated committee?

  In a recent survey, 54% of boards reported that their audit committees are responsible for IT oversight. This makes sense because audit committees typically oversee a company's risk management procedures. Only 10% of boards have a separate risk committee that is responsible for IT oversight, including cybersecurity.[23]

  There is no singular best practice in terms of committee structure. Rather, be deliberate and realistic about your organization's needs and your board's capabilities. Also, set up an opportunity to review how your board manages cybersecurity so that you can assess whether the board is continuing to meet changing conditions.[24]

- How should the board receive additional cybersecurity education to keep it abreast of business-wide threats (as opposed to training on how to personally avoid cyber-attacks)?

Again, most board members do not have—or need—a detailed grasp on cybersecurity. However, to make good decisions, directors do need continued education in emerging technologies. Most board members are very good at managing risk and recommending appropriate solutions, if they are informed. Consider devoting a portion of time each year for specific modules on your company's most common technology uses and concerns.

Along with structure, consider modes of review the board is already engaged in and how those can include (rather than set aside and silo) cybersecurity issues. If the board reviews an annual strategic plan, make sure it includes detailed, quantitative information about cybersecurity. As part of this process, the board should also approve a cybersecurity budget and consider that budget a cost of implementing the strategic plan, not as standalone IT costs.

Be sure the board and top executives have a solid understanding of how this budget is calculated and exactly what it includes. At least annually, the board should receive an updated report on the cybersecurity budget.

Some important questions for this report to address include:

- How much is spent on cybersecurity per year? Is this money spent on the most mission-critical or at-risk systems? How are these figures calculated?
- How does your budget compare to industry norms?
- What percentage of the company's annual revenue is spent on cybersecurity?
- What is the ratio of your cybersecurity team to the number of overall employees and the number of IT employees?
- How much has the cybersecurity budget increased over each of the past three years?
- What is the planned cybersecurity budget growth over the next three years?

The board should also ensure that the cybersecurity budget is under the direct control of the person held accountable for cybersecurity.

Finally, boards are experienced at using standard comparative metrics (such as profit margin, stock price-to-earnings ratio, etc.) to evaluate aspects of the business on a year-over-year basis. The board can similarly develop and monitor specific metrics to assess cybersecurity on an ongoing basis. These measures might include:

- Amount of "dwell time" (i.e., the amount of time it takes to discover and end an attack)
- The percentage of attacks that are currently being prevented and how that percentage can be improved over time
- The costs—in both time and money— of replacing a critical business function after an attack
- Patching ability: Number of days servers are out of compliance
- Number of high-risk situations mitigated (e.g., cloud solutions that use only single-factor authentication)
- Number of users with privileged access to servers
- Number of policy violations identified and/or reduced

In addition to these metrics, it is critical for the CIO to relate a meaningful narrative about security that provides an accurate view of the past as well as ROI considerations for the future. This narrative needs to be related to the board in business, not technical, terms. Setting standard times for this narrative report (i.e., quarterly, semi-annually) can facilitate effective coordination and collaboration between the board and the organization's technical professionals.

Delineate a clear cybersecurity "chain of command."

The recognition that cybersecurity is not just an IT issue, but is a business problem, is a positive development, but one that also creates confusion about governance and reporting. Who should ultimately be responsible for cybersecurity, and who should that person report to? Some believe the buck stops with the CIO, while others think cyber issues should be reported directly to the CEO.

There is not one answer that fits every organization. What is important is that your organization maps out the accountability for cybersecurity, starting with the board and extending down to the specific individual tasked with making sure the business is protected from cyber threats. This person is often the CISO. As you create and document this organization chart, discuss the reasoning behind the particular reporting structure and make sure the structure accurately reflects that reasoning.

In many organizations, the CISO reports directly to the CIO. But a new trend is emerging in which the CISO is a peer to the CIO. The rationale is that a CISO can be more effective when reporting to a CEO instead of a CIO. Whereas the CIO is typically responsible for efficiency and accessibility, a CISO is responsible for finding security vulnerabilities. These objectives and responsibilities might best be seen as parallel rather than vertical.

> "Cybersecurity professionals should not be compensated or evaluated based on how innovative their approaches sound, but on their ability to craft and execute a long-term plan that encourages the team to follow through on necessary actions."

Some organizations even have the CIO report to the CISO. The most well-known example of this is Booz Allen Hamilton, a military and business management consulting firm. It restructured its reporting lines to better reflect the company's philosophy that security must take into account all systems' operations. The company also believes that positioning the CISO at the top of the reporting line confers more visibility and prestige. A spokesperson explains that the company wanted to bring "the server room in the backroom into the visibility of senior managers."[25] This remains an unconventional arrangement, but some analysts foresee a division of responsibility in which the CISO manages the infrastructure that makes the network run and the CIO owns the applications that run on that infrastructure.[26]

Regardless of the CISO's reporting structure, a new kind of CISO is clearly gaining prominence. Traditionally, the role was filled by individuals whose experience was almost exclusively based in IT. Increasingly, CISOs have broader business backgrounds that enable them to evaluate risk relative to business value and communicate effectively across the organization.

Finally, if your company handles significant amounts of personal information, you might also consider appointing a Chief Privacy Officer (CPO). A CPO specializes in the handling of personal data, including the laws and industry standards that regulate the use of that data. This individual can identify privacy concerns, improve company policies, and increase awareness surrounding privacy issues.

Staffing and compensation should reflect the importance of cybersecurity.

In addition to reviewing your reporting structure, examine how your CIO and other top cybersecurity professionals are reviewed and compensated. Too often, speed of delivery and minimizing costs are overemphasized in cybersecurity professionals' performance reviews. Cybersecurity takes time and caution, and it can be quite costly. You do not want to encourage your staff to cut corners in order to win company accolades and hefty bonuses.

Most security work is not glamorous, and cybersecurity professionals might be attracted to more exciting solutions that challenge or enhance their knowledge set. To put it another way, they can get distracted by new technology, even though best practices often still rely on tried-and-true methods like regularly installing patches, properly configuring a network, and keeping a tight control on user credentials. Cybersecurity professionals should not be compensated or evaluated based on how innovative their approaches sound, but on their ability to craft and execute a long-term plan that encourages the team to follow through on necessary actions. If your cybersecurity team is falling short on these fundamental processes, it is incumbent on your company leadership to ask, "What in our company culture has led them to believe that it is okay—or even valued—to neglect these basic measures?"

Bring company leaders together in a cybersecurity council.

Business unit leaders should also have input into the cybersecurity risk management process. Create a cross-departmental cybersecurity council that includes the Chief Risk Officer, CPO, CISO, business unit leaders, and even outside consultants or key vendors. This can help ensure that the entire organization understands and values cybersecurity issues.

This working group can be tasked with more fine-grained details related to cybersecurity, including the creation of a Plan of Action and Milestones (POAM), a formal report recommended in the NIST cybersecurity framework. The purpose of a POAM is to identify, assess, prioritize, and monitor vulnerabilities across the organization and develop plans for addressing those weaknesses. This document details the necessary resources to accomplish the plan, milestones for achieving the requisite goals, and scheduled completion dates. Due to the broad perspective necessary for an effective POAM, it is important to have a cross-departmental team craft this document.

Principle Three:
Your employees are your biggest risks

Though we often think of nefarious cybercriminals who attack networks from faraway locations, the greatest threats typically come from within an organization. In fact, in the 2016 Cyber Security Intelligence Index, IBM found that 60% of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved unknowing accomplices.[27]

Reports of user behavior can be discouraging. In a Vanson Bourne survey, IT employees were actually more likely than average to engage in risky cyber behaviors, such as opening attachments, downloading third-party apps without authorization, and clicking on links in social media sites.[28]

Such findings could cause executives to question the value of training. If the very employees who best understand cybersecurity still engage in risky behaviors, then how could training the rest of your staff really make a difference?

Yet Ponemon recently calculated that even the least effective anti-phishing program produced a seven-fold return on investment, and the average-performing program resulted in a 37% return on investment.[29] The study also showed that the average retention rate of practical training was 75% and that the estimated long-term improvement gained from certain anti-phishing training programs was 48%. Due to the frequency and costs of phishing attacks, this translates into a yearly cost savings of $1.80 million—or $189.40 per employee.[30]

Training can clearly make a difference, if it is done right. To develop effective training programs, you should consider the different levels of need across your organization. Employees with different levels of responsibility and knowledge need different kinds of training. Consider the following approach to three key groups:

- For cybersecurity professionals: think beyond routine training and focus on ongoing education.
- For non-IT employees: training should be frequent, engaging, and relatively short.
- For executives and directors: remember they too need training, even in "basic" security protocols.

In addition to training, each company needs to consider how to handle malicious agents within the organization. Employees may decide to steal information for a competitor, sell data or intelligence, or seek revenge on the company due to perceived mistreatment. Controlling access to company data can significantly improve your chances of catching this behavior before it causes significant damage.

Cybersecurity professionals should receive more than routine training.

With mounting pressure to meet deadlines and minimize spending, many IT managers question the need of—or simply put off—training for their staff. Instead, they might operate on the implicit belief that if they hire the right people with the right technical expertise, that those employees will somehow "keep up" with the trends in their particular fields.[31]

However, investing in cybersecurity professionals' training reaps rewards for the organization and is essential for staying abreast of current threats. In particular, research shows that technical professionals who attain certification in certain specialties, like cybersecurity, perform better and are more confident than those employees without such certification. Certified IT support employees also perform better across a range of activities, including many of the most important cybersecurity actions, such as installing updated patches, configuring computers for continuous backup, and repairing network malfunctions more quickly.[32]

Make sure you understand how your cybersecurity personnel are trained and whether certification programs could improve their performance. It is worth noting that more resources for training and professional development is the top request from IT professionals to improve their job effectiveness, and 25% express concern that they are falling behind in their skills or that their skills are becoming obsolete.[33] Due to the competitive landscape for hiring and retaining the top cybersecurity talent, it's important to offer attractive incentives that will increase retention and avoid turnover costs.

For most employees, training should be short, frequent, and based in real-world scenarios.

Encouragingly, as many as 91% of organizations provide cybersecurity training to their employees, yet 75% of those do so only at the time of hire or only as part of an annual "update."[34] Such infrequent efforts reinforce the notion that security is not really something that must be taken seriously every day. In contrast, effective cybersecurity training is provided in small, digestible units; followed up with thorough testing and reinforcement; and designed to support a culture of security by engaging employees at all levels.[35]

Many organizations are opting for training through short video segments of less than five minutes that recreate real-world situations. These are much more likely to increase engagement and awareness than day-long, classroom-style training sessions or the hefty IT training manual that is never read. Regardless of method, training should be an ongoing and immersive experience geared toward changing employees' behaviors and attitudes. Also, be wary of simply equating training with simulations. "Gotcha" programs in which employees are unwittingly tested to see if they will fall for schemes can reinforce the notion that cybersecurity isn't the responsibility of the culture, but a failure of the individual. Such simulations can send the message that employees should be ashamed of and try to hide security threats in which they might be implicated.

Your training goal should instead be to build a "human firewall" in which employees know how to respond to specific threats and feel that they are contributing to the organization's long-term health.

Upper management and board members have outsized access to data but often receive less training.

Executives and directors should not perceive themselves as being "above" training. After all, they have high levels of access to important information, and yet they often receive the least training on cybersecurity measures and may be your least monitored group of users.

"Netwrix's 2017 IT Risks Survey found that although 66% of organizations perceive employees as the biggest threat to cybersecurity, only 36% of respondents say they are fully aware of employees' actions across the network."

With the predominance of phishing and social engineering attacks, organizations must recognize that senior executives are just as vulnerable as anyone. The same emotions that prompt employees to fall for phishing schemes can also entice those at the top of the company—feelings like excitement, curiosity, doubt, or even boredom. Don't be fooled into assuming your senior team can always outwit—or sniff out—cybercriminals.

Creating specific training modules for executives can be beneficial. But keep in mind that they still need help in avoiding manipulation (e.g., phishing attempts) and letting go of bad habits (e.g., failure to update passwords). Training in everyday cybersecurity measures can help even top-level managers evaluate risks and behaviors more effectively.

Because you can't eliminate user error, you should restrict access to data.

Although training can help curb users' bad behaviors and decrease the likelihood of breaches, it remains important to prudently manage user access to data. Netwrix's 2017 IT Risks Survey found that although 66% of organizations perceive employees as the biggest threat to cybersecurity, only 36% of respondents say they are fully aware of employees' actions across the network.[36] Such findings underscore that companies need to establish stricter protocols over user activity.

Many organizations do not even maintain a solid account of who has access to what data. When they sit down to tally up this information, they are often quite surprised to discover just how many privileged users they have.

Do not underestimate the number of privileged users in your system. In fact, do not "estimate" at all when it comes to this metric. Strive instead to get accurate data from across the organization on how many users have access to what levels of data—especially your "crown jewels."

Access to data should always be allocated on a need-to-know basis, according to each employee's specific responsibilities. This does not mean simply differentiating between contract and full-time employees (FTEs). After all, an FTE can quit tomorrow—just like a contractor. So, while there are differences between contractors and FTEs, those differences are too frequently overemphasized in cybersecurity protocols.

Companies should transition away from using roles or titles to determine access to data. Role-based access control (RBAC) has not adapted well to new business applications, which are more complex and involve greater collaboration among users with various roles. Increasingly, companies are turning to attribute-based access control (ABAC), which provides access to data based on multiple user qualities. This allows for more dynamic and complex protocols. As more applications move to the cloud, ABAC can help companies better prevent insider threats, meet tighter regulations, and share information more securely.

Another tool that can help restrict user access is Privileged Access Management (PAM). This software uses monitoring techniques to identify exactly what a particular user or user account is doing at any given time, including what systems the user is accessing and if the user is able to elevate privileges. Although no one technique or piece of software is a "silver bullet," PAM may be helpful in many situations where user access can cause serious problems for the organization.

Finally, an organization must also have clear protocols to follow in the event of job changes, promotions, and terminations, which should include explicit guidance for access to networks, devices, and physical locations.[37] Management must make sure these plans are enforced and that it is clear who is responsible for executing each part of the plan (the supervisor, the IT department, the group's administrative assistant). Be realistic about who has the ability to follow through quickly and ask the CISO which steps can be automated—often the ideal method for controlling credentials and access.

Principle Four:
Detect, detect, detect

Much of this paper focuses on ways to help prevent data breaches—including training, prioritization, and treating cybersecurity as a whole-enterprise undertaking. Detection efforts often go hand-in-hand with prevention and protection strategies. Think of it like health care: we know that good preventative efforts, like vaccinations and avoiding unhealthy behaviors, can lower costs and improve outcomes. However, we also recognize that early and accurate testing can make us aware of serious issues before they become catastrophic.

Of course, there is not a one-size-fits-all solution for striking the right balance between prevention and detection in your cybersecurity strategy. The key is determining the correct approach for your company, given its particular risk profile.

The reality is that many companies have devoted more resources toward prevention than detection. To be clear, we are not suggesting that your organization abandon its prevention efforts; prevention and protection tools remain essential components of a robust cybersecurity strategy. But prevention is not enough when faced with cybercriminals who are increasingly determined and abundant.[38] As many experts caution, it is not a question of if your system will be breached, but when.[39]

A note for small- and medium-sized businesses: Do not believe that criminals are not interested in your organization because of your relatively small revenue. Your low profile also does not keep you from becoming a target. Because small businesses have smaller IT staffs, they are often easier targets, and they typically have fewer resources to detect and respond to a breach. This section includes suggestions that even small businesses can implement in order to improve their detection capabilities, as well as recommendations about when and how to outsource certain detection efforts.

Research shows that most businesses' detection efforts are woefully slow or inadequate. The mean amount of time it takes for large organizations to detect a security breach is 206 days, and as many as 71% of incidents go undetected.[40] Further, most cyberattacks are not even detected by the affected entities. In fact, 53% of cyberattacks are first identified by law enforcement or other third parties.[41]

The longer it takes to detect a data breach, the more expensive the data breach becomes.[42] When a company was able to identify a breach within 100 days or less, the average total cost of data breach was $2.80 million. When it took over 100 days, the estimated cost was $3.83 million. In short, increasing your detection capabilities can significantly reduce your total costs.[43]

Internal monitoring

To quickly detect security incidents, your cybersecurity team must have complete visibility across all technical assets, properly store and analyze logs, and be sufficiently resourced to investigate alerts in a timely manner. Although senior leadership cannot be involved in actively detecting each security problem, executives can help make sure that detection is prioritized and can create performance incentives to encourage cybersecurity reviews.

To determine whether your detection efforts need to be strengthened, executives should consider the following factors:

1. **Behavior:** Senior leadership needs a clear understanding of how the cybersecurity team identifies and tracks potentially malicious behavior. In particular, make sure that responses are consistent across the organization.

   For example, many companies have multiple web servers deployed across many applications, but each instance of that web server may be managed by different teams. Is each team monitoring for the same anomalous behavior? One team could be watching for a certain set of web server status codes, while another team watches for a different set. As a general rule, there is little, if any, reason that a certain web server status code would be considered anomalous in one instance but normal in another. At the very least, leadership should know if such divergent practices are occurring and seek a good explanation, if they are.

   To better understand how your IT staff defines and tracks behavior, determine:

   - How does your company define anomalous and/or threatening activity?
   - Does your cybersecurity team agree on what constitutes anomalous behavior, and is this definition applied across the organization?
   - How does your cybersecurity team know when anomalous and potentially malicious activity is occurring?
   - Does the cybersecurity team map normal behavior (both for human users and devices) on the network?
   - Is your team properly trained to identify anomalous activity? Are they analyzing the relevant data in your detection systems, or are they missing attacks?

2. **Alerts:** Responding to threats requires trained cybersecurity professionals who can analyze and properly respond to system alerts. Frequently, security teams are overwhelmed by alerts and understaffed to react adequately. Studies indicate that up to 70% of alerts end up not being investigated.[44] In addition, a high number of false positives can lead to a kind of "alert fatigue" among your cybersecurity department, which can result in employees missing or even ignoring potential threats.[45]

To ensure that your team responds well to alerts and that you accurately understand your team's response method, determine:

- Does your cybersecurity team have sufficient resources to respond quickly to alerts? For reference, an International Data Corporation study showed that three full-time personnel can handle 300 alerts per day, total.[46] Approximately half of security operations managers report that they receive more than 5000 security alerts per day.[47]
- What systems and software does your team use to prioritize alerts and threats?
- How does the team determine which assets and users may have been compromised?
- How does your team measure and track its response time to threats?

3. **Reporting:** In many organizations, cybersecurity professionals feel pressured to deliver results at the lowest possible cost. Because of the knowledge gap that often exists between them and senior leadership, cybersecurity professionals may treat reporting as a "pro forma" activity. Unless leadership has established clear reporting guidelines and metrics, IT personnel can hide the real results of their investigation—which many times may actually be, "We don't know." Managers may simply omit items from a report when they can't determine the definitive cause, or they may attribute the root cause to something that isn't accurate.

   Company leadership needs to identify which metrics and reports are meaningful and ensure that assessments are driven by a desire to find real causes and solutions, not simply demonstrate due diligence. Determining the appropriate reporting solution should involve a back-and-forth exchange between cybersecurity professionals and senior management, and it can take time to get right.

   To identify the most relevant metrics, seek to understand:

   - Which response metrics are reported to senior leadership? How often are these metrics reported?
   - How are the results of threat investigations reported to leadership? Is leadership notified when an investigation yields no root cause or an indeterminate cause? Are cases left "open" until a root cause is determined?
   - Does the security team have the ability to investigate fully across all technical assets? How does the security team log information that is needed to investigate a security incident?[48]
   - Does your security and compliance function report to IT, or is it part of a separate department? If the compliance function is part of IT, how do you ensure that investigations are thorough and independent, rather than geared toward making IT "look good"?
   - What external frameworks does your compliance team use to gauge your efforts? The NIST framework provides good general guidelines, and your industry may also have its own particular standards (such as HIPAA). Industry compliance standards may not guarantee that your network is completely secure, but they can provide guidance on which metrics are appropriate and useful.

Reality check: Third-party auditing

A critical component to ensuring that your threat detection is working as intended is to implement thorough and regular external audits. Time and again, it turns out that high-profile breaches could have been avoided if organizations had performed the appropriate external audits. The objective of such audits and third-party evaluations is to have an independent assessment of your organization's detection and reporting functions. There is tremendous benefit to having an independent group look at—and report on—the effectiveness of your controls.

Typically, companies undergo third-party assessments annually to determine if their security vulnerabilities can be exploited by hackers. Many industries require this approach in their compliance regulations, such as the Payment Card Industry Data Security Standard. A third-party review is very good practice and has increased corporate security, but it also has weaknesses. Often, external audits focus only on finding vulnerabilities, but they fail to determine if a particular vulnerability is currently being exploited. Thus, many companies perform their annual assessment only to experience a breach shortly thereafter that was caused by one of the discovered vulnerabilities. Unfortunately, many third-party audits do not check to see if the network has already been—or is currently being—compromised. An effective third-party review must include a thorough compromise assessment. This approach will help decrease the dwell time, which remains a major challenge in the security industry.

External security consultants can also be hired to try to penetrate your organization's assets and determine whether prevention and detection measures are working as intended. For example, many organizations now engage third parties for "red team/blue team" exercises. The "red team" is the penetration-testing professionals. The "blue team" is the detection team, which uses analytics to try to ferret out the actions of the "red team." Such exercises underscore the value of both penetration testing and analytics-based approaches. The object of these exercises is to help the organization set appropriate baselines and thresholds and to increase analysts' ability to detect security breaches and containment issues.

Relevant committees at the senior level should formally review reports generated from these exercises. In addition, establish a feedback loop so that insights from these studies are immediately incorporated into existing processes, policies, and manuals.

Tools that can improve detection

Today's detection efforts focus on identifying anomalous and suspicious activity within your company's network perimeter or at its endpoints—the remote computing devices that connect back to your primary network. The objective is to identify and then neutralize an active threat before it can do significant damage. Detection tools can be combined to provide a powerful array of solutions that can materially reduce the impact of a network intrusion or insider threat. However, these tools generate a significant amount of data, and it can be difficult for more junior professionals to separate "noise" from anomalous behavior. For this reason, it remains critical to have experienced cybersecurity professionals monitoring and interpreting the data generated by your detection systems.

Detection tools require well trained professionals

EDR, SIEM, and other technologies all require trained, experienced cybersecurity professionals to regularly analyze their outputs. So, senior management should make sure that the security team has the necessary resources to review data adequately and to respond fully.

It is also essential that cybersecurity teams agree on the proper metrics to monitor and then track those same metrics consistently across all systems. If your team isn't focused on the right threats and behaviors, then the best detection systems can be rendered ineffective.

Finally, because these tools require attention and analysis, they are often not advisable as (or necessary for) a whole system solution but are often best suited for your company's priority assets.

One such tool is Security Information and Event Management (SIEM), which comprises a group of complex systems that can help an organization ingest large amounts of data from disparate sources in real time. A SIEM can correlate and then analyze data that might otherwise seem unrelated. The result is an easily-read report that can help an organization identify issues, pivot resources properly, and get an accurate picture of security problems.

SIEM systems focus on log and event management and enable cybersecurity professionals to identify threats and understand exactly what kinds of activity have occurred. A SIEM provides more sophisticated capabilities than a traditional Intrusion Detection System (IDS). In fact, a SIEM can process IDS logs, as well as firewall, server, and even PC or mobile log files.

Many SIEM applications also incorporate advanced statistical analysis, and an increasing number are experimenting with artificial intelligence and machine learning. Some experts believe that SIEM technology will even be able to automate remediation in the future. However, for a SIEM to be effective, it must be properly configured. Senior management should work with the CISO and other cybersecurity professionals to set guidance and determine the appropriate assets to monitor.

Large public companies most commonly use SIEM systems, which are often expensive and require a team to maintain. Mid-sized and small companies have typically been priced out of SIEM solutions, but many are now using SIEM services supplied through SaaS applications, which lower the software maintenance and human resource costs.[49] Large enterprises tend to run SIEM software on-site because of the sensitivity of the data in the system.

Endpoint detection and response (EDR) tools can be used to monitor endpoint and network events by recording information in a database for further investigation and reporting. This technology compares network activity to baseline norms in order to quickly identify patterns, risky behaviors, and anomalies. EDR can be automated so that suspicious activity will immediately trigger a call for action. Many EDR applications also enable cybersecurity professionals to glean valuable insight by running their own "manual" analysis on network usage data.

Principle Five:
Data protection: collect what you need, share only what you have to

We have discussed detection before protection because detection is still relatively under-resourced in many organizations. However, as high-profile breaches have continued to garner media attention, concerns about protecting sensitive data and personal information have dramatically increased. Yet data collection is a dynamic process, and the protocols for protecting it are constantly shifting. Your organization, therefore, needs to have flexible and adaptable approaches to protect your data.

Collect only business-critical data. If you don't collect the data, it can't be stolen from you

Over and over, data is stolen from companies that have no business keeping the information in the first place. Senior executives and board members need a full and accurate inventory of the data your organization is gathering, especially if you maintain records on consumers. Along with this inventory, you must understand how this data is stored and maintained. Holding onto data past its utility increases your vulnerability without increasing business value.

It is also worth remembering that data is only useful when you process and analyze it. Collecting data that you never review but hope that you might one day make useful—a practice more commonly referred to as "hoarding"—is expensive and dangerous. When you approach cybersecurity from an ROI perspective, the costs of this approach typically far outweigh any imagined benefits.

Be wary of business unit leaders who promise that at some point in the future the organization will make competitive use of stored data. Naturally, these managers are eager to collect ever more information, but despite their best intentions, they may not have an accurate understanding of what is required to analyze and store it. After all, it is very rarely their responsibility to maintain and secure it. Determining what data is truly mission-critical and worth the risk is, therefore, necessarily a senior-level decision. Make sure your organization has clear plans and a realistic estimate of the resources required to collect, store, protect, and analyze the data you keep.

Vendor and supply chain vulnerabilities

Following the notion that you should only collect data that you will use for mission-critical goals, apply a similar check on the data you share with vendors. If you don't give third-party suppliers access to your data, those suppliers can't compromise it without your knowledge. Remember to apply the "minimal access" rule to vendors, just as you do to employees. Weigh carefully what data vendors need and limit their ability to access your data.

Also, keep in mind that, legally, if your organization owns the data, then you are responsible for its security, not your vendor. Consider the consequences of suppliers providing access to the data that they can access, which might include intellectual property, customer-to-employee data, commercial plans, or contracts and legal documentation. It is no surprise that many companies are more carefully scrutinizing their vendor relationships and demanding greater transparency from their third-party suppliers.[50]

Some risks to consider when working with third-party suppliers include:

- Access to physical spaces, networks, codes, etc., that enables employees to damage your organization.
- The use of compromised hardware or software.
- Inadequate data protection controls.
- Access to company premises during off hours when surveillance is low.
- Poor information security processes from lower tier suppliers.

The "suppliers of your suppliers" should be of particular concern to your organization, constituting what some refer to as your "chain of trust." If your third-party supplier has a relationship with another supplier, then be sure that you all have the same agreements and standards in place. Attackers commonly target a lesser-defended vendor in order to gain access to the principal enterprise network. Your organization is only as secure as its weakest link, and you are linked all the way down to your suppliers' suppliers.

When it comes to vendors you already work with, make sure you understand what data they can access and how they gain access to it. Task your security team with mapping the different assets that suppliers have access to. Then, determine which controls protect those assets. Finally, stipulate how your different third-party suppliers will be involved should there be a threat or a breach. This mapping exercise may best be handled by the cross-departmental cybersecurity committee, as business unit heads might be aware of third-party suppliers that technology professionals are not.

When choosing new vendors, stipulate your cybersecurity requirements in your RFP before you even begin the selection process. Before signing a contract with a new supplier, conduct an external audit to ensure that the supplier meets your standards and actually follows the security measures they promised. Such audits should ideally be repeated at least annually. In some cases, audits may also need to be event driven—for example, if the vendor supplies a new service that affects your company's "crown jewels" or if the vendor has recently been purchased.

Your security requirements should also be reiterated again in any service-level agreements (SLA). SLAs should clearly state metrics and delineate responsibilities so that parties act in mutual understanding. Some cybersecurity components to consider, including in an SLA, are:

- That vendors meet your necessary industry compliance standards, such as HIPAA.
- The right to monitor the vendor's systems and enact countermeasures before attacks can move onto your network.
- A "one strike and you're out" policy for products that do not meet requirements or are counterfeit.
- Legacy support for end-of-life products and platforms.
- Assurance that component purchases will be made through approved vendors only.
- A process for monitoring vendor access to your network and regular meetings to review those logs.

Changing legal environment will make keeping up with regulations difficult

New legal requirements are also changing the data protection landscape, increasing the expectations for consumer privacy, as well as the cost of compliance. Most notably, in May 2018, the new European Union rule governing consumer privacy, the GDPR, will go into effect. This law restricts how companies can use and migrate personal information and imposes steep fines for infractions (up to almost $24 million). It applies not only to companies that operate in the EU but also to all companies that process the personal data of EU residents, which means that companies from around the world will need to adjust how they store and protect personal data.

Regulation/Law	Region	Date of effect	Important Points
General Data Protection Regulation (GDPR)	E.U.	May 2018	• Requires companies to provide a "reasonable" level of data security • Imposes strict standards for reporting breaches • Makes it possible to hold companies liable for third-party vendor data mishandling • High-level fines could reach up to £20 million or 4% of company revenue
Feb 2018 SEC Guidance	U.S.	February 2018	• Emphasizes the need for executives at public companies to be more involved in cybersecurity risks and incidents • Stresses the urgency for public companies to make appropriate disclosure to investors • Details the growing concerns about unlawful trading surrounding data breaches

Regulation/Law	Region	Date of effect	Important Points
Notifiable Data Breach	Australia	February 2018	• Expands number of organizations required to keep personal data secure • Implements new reporting standards for data breaches • Allows for penalties up to A$1.8 million
Cybersecurity Law	China	June 2017	• Requires network operators to store certain kinds of data in China • Allows Chinese authorities to conduct spoto-checks • Has raised concerns about increased data controls and risks of intellectual property theft

In the U.S., in 2017, New York began requiring financial services companies to perform comprehensive cybersecurity assessments, and in early 2018, the SEC followed suit by releasing new guidance that called for increased disclosures to investors. Notably, this guidance calls on boards of directors to explain how they fulfill their "risk oversight responsibility in this increasingly important area."[51] Finally, in the wake of the Equifax breach, several states, including Colorado and Nebraska, have introduced laws calling for greater protection of consumer data and financial consequences when there is a failure to do so.[52]

New laws are also being implemented across Asia, most notably in China, South Korea, and Hong Kong. In early 2018, an Australian law went into effect that requires businesses to notify the Australian Information Commissioner and affected customers of serious data breaches.

Keeping up with these ever-changing regulations is an ongoing task that is not likely to slow down any time soon. For this reason, it is prudent to make one executive responsible for understanding all legal and regulatory requirements surrounding cybersecurity in every jurisdiction where your company operates. This individual should also help determine how these requirements are incorporated into your cybersecurity strategy.

Principle Six:
Develop robust contingency plans (and test them!)

If recent attacks have taught executives and directors anything, it is that your organization's response will shape how the media, the public, and your customers interpret the breach and your culpability.

If your company has not created a formal incident response team, this is a critical component of a cybersecurity strategy. In fact, the presence of a formal team has been shown to reduce the cost of a security breach by $19 per compromised record, on average, and a strong team can generate savings of almost $125 per record.[53]

In addition to having formal procedures in place, you must frequently and vigorously test your company's response plans. If you want to mount a successful response when a real breach occurs in real time—a time that will certainly be high stress—you need to practice.

Create internal crisis management playbooks

To create a good response playbook, you need to recognize that all threats and attacks should not be handled in the same way. Prioritize the most likely cybersecurity threats and create the most robust and detailed plans for those scenarios. For each of your biggest risks, determine which key players in your organization will lead the response, and these people should each create a tailored response plan relevant to their particular threat.

Effective response plans should include workflows for every scenario and a detailed chart that clarifies the roles and responsibilities of all stakeholders. The person responsible for crafting the plan should also make sure that team members understand their roles and what deliverables and actions are expected from them. Consider including checklists or reports that can be quickly completed in times of difficulty. Some companies create internal call guides, which indicate who needs to be contacted, identify who will initiate crisis management calls, and provide templates for those calls' agendas and follow-up reports. As these plans are created, make sure they include key departments across your organization, including legal, communications, marketing, and human resource departments, depending on the kind of threat considered.

Executives and board members must be directly involved in drills and simulations

Surveys indicate that as many as two-thirds of organizations do not adequately involve stakeholders in cybersecurity incidents and lack clear escalation paths for involving senior management.[54] Given that it took Equifax's (former) CEO weeks to learn about the massive breach at his company, you must seriously consider the consequences of failing to report up the chain of command.

Senior leadership should work with the organization's cybersecurity professionals to determine how executives should be notified of and involved in potential cybersecurity incidents. Questions to answer include:

- When should directors be informed of a potential crisis situation? It is tempting to answer this question with, "as soon as one is discovered," but this may not be realistic or necessary. It might be more advisable to wait until a threat is verified or perhaps even resolved.
- Should the severity of the incident trigger different responses? For example, do senior executives need to know about every kind of threat immediately? Can some instead be included in the regular reporting? Do some kinds of threats warrant specific kinds of communication?
- Does your industry have any specific requirements for when you need to report a threat or attack?[55]

Once it is determined how executives will be involved in threat responses, make sure senior leaders take an active, yet supportive, role in drills and tests. Leadership's involvement must project the right attitude: encourage collaboration, respond smoothly, and support a calm, flexible environment. Follow-ups should not involve blame—especially not personal blame—because this will encourage employees to lie or hide what occurs when a real crisis transpires. Instead, make clear that these tests are intended to reveal systemic issues so that the organization can improve—through better training, more robust systems, or revised processes. The board should also have the opportunity to weigh in and ask questions concerning any reports given about company drills and simulations. These questions should be addressed in a formal session by the board or at the very least in a dedicated portion of a regular board meeting. Such meetings greatly help in making sure the "back and forth" discussion between the board and cybersecurity professionals is taken seriously. It also amply demonstrates an attitude of care and due diligence.

Always keep in mind that your role as a leader is to help, not hinder, the organization's ability to respond to a crisis, so whatever "value" you add to the process should be focused and minimal. Let business unit leaders and cybersecurity professionals have the opportunity to demonstrate their expertise and abilities during drills and tests.

Plan external engagement and outreach—learn from Equifax

The Equifax breach provides a seemingly endless list of how not to handle a cybersecurity crisis—failure to address a known vulnerability, delaying disclosures, misdirecting victims, and lying about the full extent of the breach. Learn from that company's mistakes. In the event of an attack, strive for transparency and simplicity—internally and also externally.

You must consider in advance how to involve legal counsel and your PR team early in your response. A delay in contacting your legal team risks compliance failures and potential lawsuits, and repeatedly, slow or weak public statements have damaged prominent companies' reputations.

"A delay in contacting your legal team risks compliance failures and potential lawsuits, and repeatedly, slow or weak public statements have damaged prominent companies' reputations."

When preparing your external responses, task your legal counsel to determine when in the process you will notify law enforcement. Within the U.S., as of now, there is no national data breach notification law, so various federal and state laws and regulations determine who must be notified. In most cases, you need to follow laws in the place where your company is domiciled as well as laws in the places where your customers reside. Determine which regulatory agencies you are governed by and make sure you understand—and are prepared for—their notification requirements. Keep in mind that some requirements are straightforward and well known, while others are complicated or obscure.

When considering how to communicate externally, remember that the public's response does not always match the seriousness of threat. You cannot dictate how the media reports the story, and therefore you cannot control how the public will interpret it. Cyberattacks often involve multiple technologies and organizations, but nuance and complexity are typically "streamlined" in brief news pieces intended for a general public with little technical knowledge. You may know that the breach is not the result of a serious, ongoing vulnerability, but the public may not understand that. Treat all breaches as serious and emphasize your organization's responsiveness.

A thoughtful communications plan is essential. Your PR professionals must help craft this plan so that you can leverage their experience before the breach, rather than in the midst of it. The communication plan should identify a rapid response team, including a clear chain of command and a designated spokesperson. Your employees must know who is in charge and who has final approval over statements and press releases. You should also clarify who in the organization will draft the official explanation and reaction to the breach—language that can then be used across press releases, interviews, and disclosure statements. All messages should strive for honesty, simplicity, and consistency.

The communications plan might also include different templates for external reporting, since most significant breaches require disclosures to regulators, shareholders, and others. This will make the process more efficient and responsive. Some businesses even go so far as creating a website, inaccessible to the public until after an attack, that contains key information and tools to address the breach. This enables them to begin communicating immediately after a breach has been verified.

Communication becomes especially important when handling breaches that involve private consumer data. Consumers are conditioned to believe that companies are cavalier with and unconcerned about their privacy. Be sure that senior executives pay particular attention to communication plans involving these incidents. A consistent, clear, and immediate response can go a long way toward rebuilding the relationship with your customers, regulators, and the public more broadly.

Conclusion

Most executives recognize the importance of cybersecurity, but many still approach the topic with trepidation—and even fear—rather than seeing it as an opportunity for the company's leadership to grow and for the culture to evolve.

Assuredly, part of this uncertainty stems from the "knowledge gap" that exists between senior leadership and cybersecurity professionals. More and more, though, organizations are building corporate cultures that encourage collaboration and mutual support between the technical experts and the company's leadership. Boards are appointing directors with extensive technical knowledge and experience, and they are creating new reporting structures and committees that can more regularly engage in guiding cybersecurity strategy. Likewise, successful cybersecurity professionals, especially CIOs and CISOs, are gaining broader managerial experience before entering their leadership positions. This enables them to speak to executives using the language of business strategy, rather than in exclusively technical terms. In short, leading companies are making progress in closing both the knowledge gap and the communications gap.

This is an important development, given the evolving cybersecurity landscape. It is becoming increasingly clear that companies can no longer delude themselves into thinking they can be perfectly protected against every possible attack. It is not a question of "if" you will be attacked, but "when." As criminals find more targets to attack and more ways to leverage malware and other malicious tools, defenses will have to be ever more coordinated across an organization. Ongoing training, well-resourced detection efforts, and detailed response plans can help prepare organizations for an eventual breach.

To transform your company culture so that it truly embraces cybersecurity, senior leadership must view it as part of the broader risk management process, rather than jettisoning it off as a technology problem with a technology solution. Instead of blaming individuals for issues, always look first to the corporate structure. Are employees encouraged to hide mistakes, or investigate and address issues? Is your cybersecurity department adequately resourced to address challenges, or is the team encouraged to cut corners and deliver at ever-increasing speeds with an ever-depleted budget? The most successful cybersecurity approaches are not necessarily the most expensive, but they do require persistence, attention, and prioritization. These are the attributes that only senior leadership can bring to an organization.

References

1 John Drzik, "Cyber Risk is a Growing Challenge. So How Can We Prepare?" World Economic Forum: https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready

2 Steve Morgan, "Top 5 Cybersecurity Facts, Figures and Statistics for 2018," CSO, January 23, 2018: https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

3 SpencerStuart, 2016 Global Board of Directors Survey, p. 5.

4 Michael Bloch, Brad Brown, and Johnson Sikes, "Elevating Technology on the Boardroom Agenda," McKinsey & Company, October 2012: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/elevating-technology-on-the-boardroom-agenda

5 PwC, "Directors and IT: A User-Friendly Board Guide for Effective Information Technology Oversight," p. 18.

6 Nate Lord, "Social Engineering Attacks: Common Techniques and How To Prevent An Attack," DataInsider, January 15, 2018: https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

7 "How to Protect Your Networks from Ransomware," p. 2: https://www.justice.gov/criminal-ccips/file/872771/download

8 Steve Morgan, "Ransomware Damage Report," Cybersecurity Ventures, May 2017: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

9 Patrick Howell O'Neill, "Ransomware is Now a $2 Billion-Per-Year Criminal Industry," CyberScoop, November 21, 2017: https://www.cyberscoop.com/ransomware-2-billion-bitdefender-gpu-encryption/

10 McAfee Labs, 2018 Threats Prediction, November 2017.

11 To see the 2017 report, visit: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

12 For IBM's Breach Calculator, visit: https://databreachcalculator.mybluemix.net/. A list of additional calculators can be found here: https://www.privacyrisksadvisors.com/data-breach-toolkit/data-breach-calculators/.

13 Steve Morgan, "Cybersecurity Market Report," May 2017: https://cybersecurityventures.com/cybersecurity-market-report/

14 Another example is the SEC's citation of R.T. Jones Capital Equities Management. The company was cited after a data breach because it failed to put policies and procedures into place relating to cybersecurity. The SEC ruling specifically faulted R.T. Jones for failing to put cybersecurity policies in writing.

15 For example, a suit was brought against Wyndham Hotels directors and officers in 2014 for data breaches that occurred between 2008 and 2010. The court dismissed the suit in large part because the board was able to demonstrate that members sufficiently supervised the company's cybersecurity preparedness. the judge cited the frequency and depth of board discussions of cybersecurity. Because the board could demonstrate sustained attention to cybersecurity (including regular meetings and reports), it was found to have upheld its responsibility. In a similar case against Home Depot's board in 2016, the court ruled that the board's decisions only needed to be "reasonable, not perfect." Citing Delaware case law, the judge reasoned that, in order to prove bad faith, the plaintiffs needed to show that the board took no steps to prevent or remedy the situation and that directors "knowingly and completely failed to undertake their responsibilities." The Home Depot directors did not shirk their responsibilities as a board so were not judged to have acted in bad faith.

16 This site contains several good formulas for assessing the ROI of a phishing simulator: http://resources.infosecinstitute.com/phishing-simulation-how-do-you-calculate-effectiveness-and-roi-part-2-of-2/#gref

17 NIST Cybersecurity Framework, p. 11.

18 World Economic Forum, "Advancing Cyber Resilience: Principles and Tools for Boards," p. 4

19 https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

20 PwC, "Directors and IT: A User-Friendly Board Guide for Effective Information Technology Oversight," p. 17.

21 PwC, "Boards Confront an Evolving Landscape," p. 2.

22 SEC Commissioner Luis A. Aguilar cited this approach in his speech, "Board of Directors, Corporate Governance, and Cyber-Risks: Sharpening the Focus," June 10, 2014; https://www.sec.gov/news/speech/2014-spch061014laa#_edn37

23 PwC, "How Your Board Can Decide if it Needs a Risk Committee," https://www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/board-risk-committee-needs-assessment.html

24 For more about board structure and cybersecurity concerns, see Lawrence J. Trautman and Kara Altenbaumer-Price, "The Board's Responsibility for Information Technology Governance," John Marshall Journal of Computer & Information Law, October 22, 2011; revised: December 24, 2017.

25 Eric Chabrow, "Role Reversal: CIO Reports to CISO," BankInfo Security, April 7, 2014: https://www.bankinfosecurity.com/blogs/role-reversal-cio-reports-to-ciso-p-1648

26 Jeffrey Guy, "The CIO Will Report to the CISO," Carbon Black, July 21, 2017: https://www.carbonblack.com/2017/07/21/cio-will-report-ciso/

27 IBM X-Force 2016 Cyber Security Intelligence Index, p. 11.

28 Maria Korolov, "Does Security Awareness and Training Even Work?" Wombat Security, September 30, 2015: https://www.wombatsecurity.com/news/does-security-awareness-and-training-even-work

29 Maria Korolov, "Does Security Awareness and Training Even Work?" Wombat Security, September 30, 2015: https://www.wombatsecurity.com/news/does-security-awareness-and-training-even-work

30 Ponemon Institute, "The Cost of Phishing and Value of Employee Training," August 2015, p. 3.

31 CompTIA, "IT Support and Security Performance," p. 1.

32 CompTIA, "IT Support and Security Performance," p. 5.

33 CompTIA, "Career Insights Study."

34 Aberdeen Group, "Security Awareness Training: Small Investment, Large Reduction in Risk," p. 2.

35 CompTIA, "The Evolution of Security Skills," April 2017.

36 Netwrix, "Just 26% of Organizations are Ready to Handle IT Risks, Reveals Netwrix Survey," June 13, 2017: https://www.netwrix.com/just_26_per_cent_of_organizations_are_ready_to_handle_it_risks_reveals_netwrix_survey.html

37 If you do not have a plan in place or need to update your plans, you can find a good checklist here: https://www.delcor.com/resources/blog/a-hr-and-it-checklist-for-termination-of-employment

38 Nate Lord, "Cyber Security Investments: Experts Discuss Detection Vs. Prevention," DataInsider, July 27, 2017: https://digitalguardian.com/blog/cyber-security-investments

39 Brian NeSmith, "Why Cybersecurity Is About More Than Prevention-Focused Products," February 28, 2018: https://www.forbes.com/sites/forbestechcouncil/2018/02/28/why-cybersecurity-is-about-more-than-prevention-focused-products/#63cb5eab7408

40 Tim McCollom, "The Cybersecurity Imperative," Internal Auditor, July 31, 2015

41 Larry Clinton, National Association of Corporate Directors, "Cyber-Risk Oversight," p. 5.

42 Ponemon Institute, "2017 Cost of Data Breach Survey," p. 6.

43 Marianna Noll, "2017 Ponemon Cost of Data Breach Study: Analyzing the Research," IT Security Central, November 28, 2017: https://itsecuritycentral.teramind.co/2017/11/28/2017-ponemon-cost-of-data-breach-study-analyzing-the-research/

44 Kevin Broughton, "Automated Incident Response: Respond to Every Alert," Swimlane, March 3, 2017: https://swimlane.com/automated-incident-response-respond-every-alert/

45 Ryan Francis, "False Positives Still Cause Threat Alert Fatigue," CSO, May 3, 2017: https://www.csoonline.com/article/3191379/data-protection/false-positives-still-cause-alert-fatigue.html

46 Bill Sweeney, "Cutting through the Noise: How to Manage a Large Volume of Cyber Alerts," SecurityWeek, January 11, 2016: https://www.securityweek.com/cutting-through-noise-how-manage-large-volume-cyber-alerts

47 Cisco, Global 2017 Security Capabilities Benchmark Study

48 For additional questions and issues, see the NACD, "Ask Your Security Team These Questions in 2018," January 16, 2018: https://blog.nacdonline.org/2018/01/ask-your-security-team-these-questions-in-2018/

49 For a lengthier discussion of choosing SIEM software, see CSO, "What is SEIM Software? How It Works and How to Choose the Right Tool," November 28, 2017: https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html

50 For more on supply chain considerations, see National Institutes of Standards and Technology (NIST), "Best Practices in Cyber Supply Chain Risk Management," https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf

51 Security and Exchange Commission, "Commission Statement and Guidelines on Public Company Cybersecurity Disclosures," p. 18.

52 For more information on U.S. cybersecurity legislation and recent cybersecurity cases against boards of directors, see Paul Gupta, "Cybersecurity: What Every Board Should Know and Do," FinTech Law Report, January/February 2018.

53 Ponemon Institute, "2017 Cost of Data Breach Study," p. 6.

54 Kelly Bissell, Ryan LaSalle, and Kevin Richards, "The Cyber-Committed CEO and Board," Accenture, p. 9.

55 For more details on involving the board members in cybersecurity threats, see NACD, "Seven Steps to Minimize Fallout from Crisis Situations," February 1, 2018: https://blog.nacdonline.org/2018/02/seven-steps-crisis-situations.

Appendix A
Cross Reference to NIST Framework Sections

"Building a Culture of Cybersecurity" highlights six core principles to help board members and executives focus on the most important or overlooked aspects of a cybersecurity strategy. These principles are built upon the NIST Framework's more comprehensive—and technical—guide for creating a complete, top-tier cybersecurity strategy.

The table below provides a cross-reference between the NIST Framework and "Building a Culture of Cybersecurity." As your team works to bolster your cybersecurity efforts, we encourage you to consult the NIST Framework for additional information, metrics, supporting materials, and guidance. Following each principle in "Building a Culture of Cybersecurity," you will find a list of the relevant "Categories" and "Subcategories" from the NIST Framework.

Principle	Identify	Protect	Detect	Respond	Recover
1. Integrate cybersecurity into your business strategy	ID.AM ID.RA-1 ID.RA-5 ID.BE-3 ID.BE-4 ID.RM-2				
2. Your corporate structure should reinforce a culture of cybersecurity.	ID.AM-6 ID.GV-2	PR.AT-4			
3. Your employees are your biggest risks.	ID.RA-1	PR.AC PR.AT-1 PR.AT-4			
4. Detect, detect, detect.		PR.AC-1; PR.DS-6 PR.IP-7	DE.AE-2 DE.CM-1	RS.AN-1; RS.AN-3; RS.MI-3	
5. Data protection: collect what you need, share only what you have to.	ID.AM-3 ID.BE-1 ID.GV-3	PR.AC-2 PR.AC-3 PR.AC-4 PR.AT-3 PR.DS-2 PR.IP-6 PR.IP-7 PR.PT-3			
6. Develop robust contingency plans (and test them!).	ID.GV-4	PR.IP-9 PR.IP-10		RS.CO RS.IM-1	RC.IM-1 RC.CO

Appendix B
How to Identify Your Company's Crown Jewels

Crown jewels are typically just a small fraction of the data that a company maintains—the ".01 to 2% of data that determines whether your enterprise will survive and thrive." Estimates indicate that 70% of the value of publicly traded companies is located in their critical data, their crown jewels.[1]

Many companies operate with a tacit understanding of which data is most important, but until you explicitly identify your crown jewels, you cannot be sure that there is consistent agreement on the issue. Without this, it is impossible to know that you are prioritizing your mission-critical data.

Different companies have different crown jewels, depending on their industry, competitive positioning, and even geographic location.

Examples of Crown Jewels

Intellectual property	Designs, technical specs, proprietary algorithms
Administrative documentation	Strategic plans, contracts, new product launches
Financial analysis	M&A database, accounting records, transaction records
Data collection	CRM, employee data, consumer information

Steps for identifying crown jewels:

(1) Start with the business and its competitive advantage. Executives and board members are focused on the "big picture" and as such are uniquely responsible for developing, understanding, and maintaining the company's competitive advantage. The cybersecurity team, in contrast, is responsible for developing, understanding, and maintaining the processes and systems that protect data and assets. As a result, cybersecurity professionals tend to start the data classification process by inventorying applications, systems, and databases, and then they develop a view of risks. This is especially the case when the cybersecurity team is part of the larger IT department.

By starting this process by analyzing your business's context and distinctiveness, you can more effectively identify which technical assets are truly critical to sustain the business over the long term. The effort should be grounded in a view of the business and its value chain.

(2) Consider your strategic plan and business objectives. Keep in mind that your most important data may not be clearly tied to your main business operations. Do not only think in terms of your industry and its core practices; think in terms of the strategic plan for your particular business.

For example, imagine a healthcare provider that makes patient data its only priority. It could be neglecting other assets, such as confidential financial data relevant to important negotiations. This is a company that is not focused on its specific goals as an organization, but is instead focused on regulatory requirements.

Another example: an oil and gas company might prioritize its production and exploration data but fails to separate its proprietary information from publicly available information. Thus, the organization is using its own resources to protect public information when it should pay attention to high-value data like business negotiations and internal communications about future production sites.

(3) Understand the consequences of a breach. A helpful way to determine the value of your data is to understand what could happen if your data was leaked or lost. Would the loss of certain data eliminate your competitive advantage, incur criminal or regulatory charges, or erode your corporate brand? If particular types of data got into the public domain, how would it expose your customers, partners, or suppliers?

You will need to consult with other segments of the organization, such as the legal department and the CISO's team, to get a complete picture of these consequences. This includes a thorough understanding of regularly requirements and how to meet them.

But it is a critical part of senior managers' responsibility to actively guide these discussions, document the findings, and identify the most important data.

(4) You must be engaged in an ongoing process. Developing a company-wide understanding of your crown jewels is an important step for improving data security. However, senior managers and board members must understand that it is a continuous process, not something that can be done once and forgotten. You must continue to lead the ongoing process of data classification and prioritization. If the business loses sight of where its crown jewels are or how its data collection is evolving, then it risks returning to square zero—or that time when none of the data was clearly and consistently classified.

Identifying the crown jewels is just one part of a larger process of enterprise-wide data classification. You can learn more about the entire data classification process in the "Identify" stage of the NIST Framework. The sequence outlined above focuses more on how executives and board members in particular should be involved in identifying their organization's crown jewels.

1 Erkang Zheng, "Critical Data Discovery: Embarking on a Digital Treasure Hunt," Security Intelligence, May 13, 2014: https://securityintelligence.com/critical-data-discovery-digital-treasure-hunt/.

Acknowledgements

This work would not have been possible without the leadership, input and support of the CompTIA Cybersecurity Advisory Board. Our board members are:

Mary Beth Borgwing, President & CEO, Standish Cyber Corp

Mary Chaney, Attorney, The Law Offices of Mary N. Chaney, P.L.L.C

Jen Elis, Vice President of Community and Public Affairs, Rapid 7

Dave Fedorchak, Senior IT Program Manager

Greg Garcia, Executive Director, Healthcare and Public Health Sector Coordinating Council

Paul Gupta, Partner, Intellectual Property, Information & Innovation Group, Reed Smith LLP

Jim Harvey, Partner, Leader Data Privacy and Security Practice, Alston & Bird

David Hoid, Chief Information Security Officer, Early Warning Services

Sean Manning, Senior Professional Staff, The Johns Hopkins University Applied Physics Laboratory

Corey Schou, University Professor of Informatics, Professor of Information Systems, Associate Dean, College of Business, Idaho State University

Ari Schwartz, Managing Director of Cybersecurity Services, Venable, LLC

Corey White, Vice President of Worldwide Consulting Services, Cylance

Bill Wright, Director, Government Affairs & Senior Policy Counsel, Symantec

CompTIA Worldwide Headquarters
CompTIA Member Services, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515

630.678.8300

CompTIA.org