CROWDSTRIKE

Getting On Board with Cybersecurity

Table of Contents

"Cybersecurity isn't just a technology problem: It is a business problem — boards need to know the right governance, processes and tools are in place and have strong recovery plans in the event of a breach. They also need to ensure the related policies and practices are consistent and shared across the CISO, CIO and CRM."

Dennis O'Leary
Director on multiple boards and CrowdStrike board member

Foreword

The idea that cybersecurity is a board-level concern is not new. Private companies and their computer networks have been the target of cyberattacks for decades. This is because they generate the intellectual property, store the financial data and operate the critical infrastructure that threat actors have traditionally sought to compromise.

What is new is that data theft may no longer be their primary cybersecurity concern. The uptick in destructive attacks in recent years, highlighted by the WannaCry and NotPetya outbreaks last year, has changed the calculus. What was once a material risk is now an existential one. Cybersecurity has become an integral part of organizational risk assessment and management.

In my role at CrowdStrike® and as a faculty and a board leadership fellow at the National Association of Corporate Directors, I have noticed a change in how board members and executives pursue involvement in cybersecurity. There is a heightened sense of urgency — an increasing desire to be proactive about addressing this risk head-on, and a recognized need to increase education, awareness and participation across industries.

But among many corporate boards, there is a lack of clarity or guidance on how to actively add value or effective supervision. The technologies are complex, the networks are vast, and striking the appropriate balance between business efficiency and security is challenging even for the most sophisticated organizations.

Board members do not need to become cybersecurity experts in order to help their companies prepare, but they do need to educate themselves. This is what this white paper attempts to do: provide a primer on the risk landscape as well as actionable tools that can help companies better manage their risk.

I joined CrowdStrike six years ago because I saw the private sector as the primary front in securing society from the same cyberthreats that I combatted at the FBI. I am heartened by the growing number of corporate boards that are joining this fight and I sincerely hope this white paper will help them succeed.

One team, one fight.

Shawn Henry
President, CrowdStrike Services
and Chief Security Officer

Executive Summary

Overseeing risk management has always been a core responsibility of corporate boards. So it's no surprise that, as both the companies and the cyberthreats they face have grown, so have the number of boards taking an interest in how their organizations address cybersecurity. They have not always had an easy time of it. Although most board members are well-versed in traditional business risks — from revenue and margins to compliance, brand image and reputation — few have expertise in cybersecurity. Thankfully, board members don't necessarily need to be cyber experts, because the fundamentals of risk management remain the same; it's only the threats and the options to mitigate them that are different.

This white paper provides a primer on those threats and tools, specifically with board members in mind. It identifies the range of threats that companies face, provides guidance on how to think about and prioritize assets for additional protection, and discusses approaches for staying abreast of changes in the threat landscape. It also provides a high-level overview of technical concepts and processes that can equip board members to engage more deeply with the practitioners and subject matter experts they rely on for guidance. Lastly, it offers three "cheat sheets": one for addressing cybersecurity proactively, one for responding to a security breach, and one for personal security measures that high-value individuals should take.

Introduction

As a member of a board of directors, individuals are often asked to provide guidance to their respective organizations – often in times of crisis. This is especially true with the advent of cybersecurity threats that have become commonplace across all industries. In addition to providing financial, operational and strategic advice, board members are often expected to have a view into technical cybersecurity areas, as well.

While it's always advantageous to offset the collective wisdom of the board with advice and guidance from industry experts, it's equally important that board members arm themselves with an arsenal of pertinent questions to ask, and red flags to monitor. This document will provide a starting point and is intended to educate board members (or anyone with similar interests) about why cybersecurity has become an integral part of board-level discussions; what you need to know about cybersecurity and how it impacts your organization; and how you can better assess your organization's cybersecurity preparedness and maturity. The appendix also includes several helpful lists that board members can reference before, during and after a cybersecurity incident, such as a data breach, as well as guidance on how to protect themselves as individuals.

A Board-Level View into Cybersecurity Concerns

The growing need to address cybersecurity at the board-level becomes clearer when you consider the following guidance from regulating bodies and advisory committees.

SEC Cybersecurity Disclosure Guidance

In 2011, the SEC issued guidance on cybersecurity incident disclosure. On February 26, 2018, the SEC updated its guidance to further emphasize the criticality of cybersecurity preparedness for public companies, advising corporate directors to consider "the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents." The guidance also included reminders about applicable insider trading obligations related to disclosures of "material nonpublic information about cybersecurity risks or incidents." While not explicitly calling for cybersecurity knowledge at the board level, the guidance does emphasize a growing list of cybersecurity topics directors must consider to effectively manage risk.

General Data Protection Regulation (GDPR)

Another example of the increased focus on data protection and its implications for cybersecurity comes from the European Union (EU). Two years after its adoption, enforcement of the General Data Protection Regulation (GDPR) began on May 25, 2018. This means that many companies around the globe are now obligated to take additional steps to protect the data of their customers and employees. While this regulation is specific to companies dealing with personal data originating in the EU or European Economic Area (EEA), its extraterritorial reach is already transforming the cybersecurity posture of organizations worldwide.

GDPR stipulates principles not only for

$25 million

of penalties is allowed if GDPR is not met

protecting commonly held personal data such as name, address, and ID number, but in fact, any unique identifier of a "natural person" (living human being) under the law. Depending on context, this may encompass geolocation, IP address and cookie information. Political, racial, sexual and genetic data points receive special protections under the regulation. Due to its breadth, companies are spending millions to comply by leveraging several variations of cybersecurity and privacy controls. Accordingly, it is important for a board to understand whether compliance money is being spent effectively and in a way that will help mitigate against the risks of being fined for GDPR non-compliance. Depending on the category and severity of a violation, penalties for non-compliance can be as significant as €20 million (close to $25 million in USD) or four percent of annual global turnover (revenue), whichever is higher.

Ultimately, the GDPR is principles-based rather than prescriptive, making it open for interpretation. There are six principles that must be followed when processing personal data, along with an underlying principle of accountability to demonstrate compliance. To prevent security breaches and lawfully process personal data, organizations must take into account the "state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk" when implementing safeguards to protect their personal data. Such language provides an opportunity for board members to offer guidance based on experiences across multiple organizations to ensure that appropriate cybersecurity protections are adopted.

NIS Directive

Another cybersecurity regulatory development is the European Union's NIS Directive, which member states were required to implement as national legislation by May 9, 2018. Focused on critical industry sectors rather than data types, the directive mandates heightened cybersecurity requirements for organizations in the energy, transport, water, health, finance and critical digital service sectors. This means that board members in such sectors must ensure that cybersecurity capabilities and practices meet these standards.

Australian Data Breach Notification

Though not a holistic cybersecurity law, Australia recently implemented the National Data Breaches scheme, raising data breach notification requirements for companies that make $3 million (AUD) or more, as well as those in specific sectors, such as healthcare. This increases the impetus for Australian organizations to adopt cybersecurity measures to prevent data breaches, as well as to develop a plan for identifying, responding to, and reporting breaches when they occur.

NACD Director's Handbook

One of the key realities of recent developments is that cybersecurity is no longer a suggestion — companies that do not protect personal data and make notifications in a timely manner are subject to substantial fines.

Appropriately, the National Association of Corporate Directors (NACD) released a Director's Handbook on "Cyber-Risk Oversight" just last year. In this 2017 document, one of the guiding principles states, "Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas." The remaining principles address the need to not merely understand cybersecurity as an IT risk, but to comprehend the legal implications of cyber risks, setting the expectation that cyber risk management frameworks are developed and understanding the types of conversations related to cyber risks that should be happening at the board level. The NACD document offers valuable insights that are augmented in this white paper, which shares CrowdStrike's unique perspective as a leader in the cybersecurity incident response space.

Reason to Be Concerned

As a board member, it's important to consider why an organization may be targeted. From its inception, CrowdStrike has embraced the maxim stating "the '*what*' is less important than the '*who*' and the '*why*.'" At its core, the intent behind this statement is that the malware and other methods used in an attack offer little from a strategic perspective. Though they represent critical details about what happened and how to remediate that individual incident, what is more important strategically is to identify the actors and motives behind an attack.

Motivations in a Cyber World

CrowdStrike considers cybersecurity threats based on the following motivations:

Within each of these categories, it's possible to outline a set of likely adversary types who execute cyberattacks with those motives in mind.

State-sponsored adversaries, for instance, typically fall into the espionage category, although there has been an uptick in destructive attacks recently, as well as financially motivated eCrime attacks by nation-state actors. Much state-sponsored espionage has focused on information that provides an economic advantage: Adversaries steal intellectual property or trade secrets from organizations outside of their country in an attempt to eliminate a skills gap, accelerate research and development timelines or otherwise gain a competitive advantage. Though they are not alone, China is often associated with these incidents. In fact, over the last several years the CrowdStrike Falcon Intelligence™ team has outlined a direct correlation between alleged China-based attacks on particular industries and the goals outlined in the most recent Chinese Five-Year Plan, which sets national goals in those same industries. However, economic espionage is just one means of gaining geopolitical advantage. CrowdStrike has also seen state-sponsored attacks target information held by private companies that may have other strategic relevance, such as the personal webmail accounts of public officials or journalists whose sources may include political dissidents.

Knowledge of who is likely to attack an organization and why helps arm board members with some of the information they need to issue guidance on the organization's defensive posture. It also prepares them to be as effective as possible in the event of a cybersecurity incident. In addition to understanding the attacker's motives, board members must have similar discussions about the perceived value of an organization's systems and data, along with a view into valuable information from strategic intelligence sources.

High-Value Asset vs. High-Value Target

Cybersecurity is all about risk management. Understanding risk through the cybersecurity lens requires a conversation around assets and targets. Organizations often use the term "high-value asset" to define those systems, applications, data sets, etc., that it views as worth more to the organization than other assets. It's the organization's own view of what the "crown jewels" are. Conversely, high-value targets are those the adversaries are looking to compromise.

Understanding this difference is important when considering how best to prepare for the inevitable cyberattacks of today. You certainly should solidify your defenses to protect your high-value assets, but don't be so short-sighted as to ignore the perceived value that others may place on different areas of your business. Similarly, the antiquated idea that "they don't care about little ol' me" should be removed from consideration by every organization with an Internet connection. Low-hanging fruit still has plenty of juice in it for the wide range of online adversaries that exist today.

Additionally, as noted in the 2017 CrowdStrike Cyber Intrusion Services Casebook, supply chain partners were the initial attack vector in 12 percent of CrowdStrike's incident response cases. This means that adversaries leveraged companies that were often smaller and less secure to gain access to their end target through a trusted partner relationship. Thus, your organization may not be the ultimate target, but you could become collateral damage as the attacker compromises your environment to reach their desired goal.

The role of the board in a discussion over what constitutes "high-value" is to help the company see the forest in spite of the trees. Because board members are not living the mission of the company daily, in most cases board members are in a perfect position to provide an assessment of value from a more objective vantage point. Additionally, many board members are selected for their vast experience across multiple organizations and industries. This provides members with an opportunity to speak from a perspective that is different from those within the organization.

One last note about high-value targets: as a member of the board, you probably are one. Threat actors often focus their efforts on an organization's senior leaders because of the influence they wield and the information they have access to. Make sure you have taken the appropriate steps to secure your own business and personal accounts, and ask your security staff for guidance on how to best protect yourself and the companies you oversee. This paper provides some information to get you started in Appendix C.

Adversaries leveraged companies that were often smaller and less secure to gain access to their end target through a trusted partner relationship

Strategic Threat Intelligence

Understanding adversary motives and placing a value on your organization's assets is often made easier when you're able to leverage threat intelligence. Cyber threat intelligence (CTI) takes on two primary forms. Tactical intelligence is information that you can use to immediately improve your defenses against known vulnerabilities and attacks. Examples include IPs or URLs, malware signatures and suspicious patterns, or other indicators that can be added to your preventative tools to stop the "known bad." Alternatively, strategic intelligence informs high-level activities that an organization can take to properly calibrate its security posture. Examples may include information about new attack methods, shifts in targeting behavior by threat actors, or political or economic events that are likely to inspire a shift in threat actor activity. This intelligence is not as simple to apply to the organization as tactical intelligence, but may ultimately prove to be more valuable because it can inform both security and business decisions.

As a board member, you may not have access to either tactical or strategic CTI by default, but your decisions should be informed by at least the strategic patterns and threats in these reports. Be sure to ask your organizations how they're incorporating threat intelligence into the day-to-day decision-making process, how it informs their understanding of the threat the organization faces, and how that threat is evolving. If this information does not currently exist within the organization, you should request a briefing from a CTI vendor such as CrowdStrike, prior to determining the appropriate risk calculations for the organization.

The Anatomy of a Cyberattack

In order to identify the appropriate set of questions to ask as a board member during a cybersecurity incident, it's vital to understand how cyberattacks vary from traditional incidents such as physical security breaches, public relations snafus or a dip in profits.

The biggest difference is that with cyberattacks, it is often difficult to ascertain when an event actually started or how far it has spread. It can be equally difficult to gain assurance that you've successfully eradicated the adversary, remediated the network, and are able to return to business as usual. This is in direct contrast to the non-cybersecurity incidents mentioned above. With each of those events, there's a known point in time when it occurred; this means the nature of the impact to the business is clear (even if the extent is not), and it's often easier to identify how the incident can be resolved.

To understand why cybersecurity events are different, it is important to understand the attack lifecycle. Sometimes referred to as the "kill chain," this lifecycle is a concept that outlines the steps an adversary takes during an attack to fulfill his or her objectives. These exact steps are not always followed by adversaries, but this is a good framework from which to understand where you are in the attack lifecycle, and as a result, what the best course of action is.

CrowdStrike looks at the attack lifecycle in terms of the following phases:

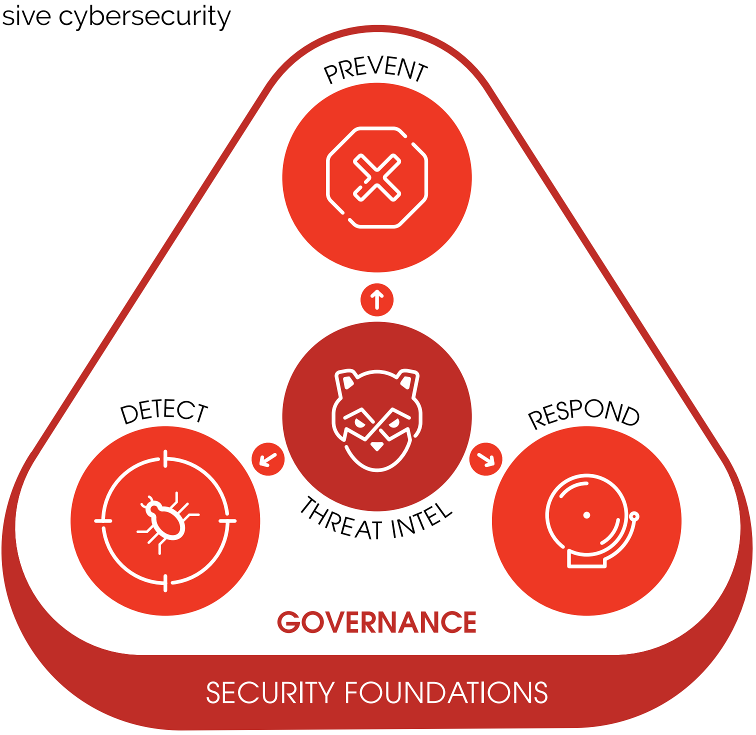
Cyber Attack Lifecycle Phase	Description
Reconnaissance	In the reconnaissance phase, an adversary researches, identifies and selects a target organization. The aim is to collect as much information as possible on the target organization.
Weaponization	The weaponization phase involves coupling a remote access tool with an exploit, to create a deliverable payload.
Delivery	The delivery phase involves transmitting the weaponized payload to the target.
Exploitation	The exploit phase occurs when a victim receives and triggers the payload, usually by clicking on a malicious link or opening the malicious attachment.
Installation	During the installation phase, the adversary establishes a persistent presence on the network through the installation of a remote access tool or other backdoor.
Command and Control (C2) Establishment	During the C2 phase, the infected victim machine beacons out to the adversary's C2 infrastructure to establish a separate, typically encrypted communication channel. This allows the adversary to interact directly with the target in what is known as a direct "hands-on-keyboard" attack phase.
Privilege Escalation	During the privilege escalation phase, the adversary explores the local system and network, looking for weaknesses that can be leveraged to gain additional, escalated privileges or credentials.
Lateral Movement	Once adversaries haves compromised the system and gained the proper privileges, they will attempt to move to additional systems on the victim's network.
Sensitive Data Exfiltration / Operatives	After the previous phases are completed, the adversary acts on its original goals and objectives. These actions typically involve the collection, encryption and extraction of the victim's valuable data.

During a cybersecurity incident response (IR) scenario, the organization will attempt to determine where the attacker is in this lifecycle. Unfortunately, most organizations are unable to detect today's adversaries until after they've exfiltrated the data they seek. This is typically due to a combination of understaffed security teams, insufficient endpoint detection technologies, and inefficient response capabilities. Additionally, CrowdStrike has seen average "breakout times" — the time it takes for an intruder to move out from it's initial intrusion "beachhead"— reduced to less than two hours, a fact which is highlighted in CrowdStrike's 2018 Global Threat Report. This doesn't provide much of a window for responders to intervene before the attacker moves from their initial entry point. For mature organizations, however, it's possible to detect an attack as it is occurring and remove attackers from the environment before they reach their objective.

Board members, therefore, should ask questions relevant to how far the adversary has progressed within the attack lifecycle. They should also anticipate a high level of uncertainty in the answers to these questions — especially early on. Once data has left the organization, an entirely new set of questions and key objectives are required. Often, by the time the board is brought into the discussion, the attack has either been contained or more likely, the damage has been done.

Assessing an Organization's Maturity

Many of the questions board members should be asking — ideally, prior to a breach — are related to the maturity of the organization's cybersecurity program. The following is CrowdStrike's view of a comprehensive cybersecurity program:



As the diagram shows, the primary building blocks of an effective cybersecurity program are the abilities to **prevent**, **detect**, and **respond**. Specifically, these core capabilities determine how well you can prevent threats from being successful, and when you can't prevent a specific threat, how quickly you can detect it and respond accordingly. These capabilities also incorporate different levels of reliance on people, processes and technology. You need trained people to conduct the necessary activities, they need to follow defined processes, and you must leverage effective technologies.

At the center of these activities lies **threat intelligence**, which can be used to increase detection, prevention and response capabilities, through the direct application of tactical indicators and by supporting thoughtful consideration of strategic concepts. For example, threat intelligence is helpful as part of the response function, because it allows you to understand who is attacking you and why. This provides for a more targeted response process, while developing and applying indicators to stop the adversary and prevent additional compromise can help shorten the incident timeline. If prevention, detection and response are the frame and engine of the car, threat intelligence provides the GPS, giving you directions of where to go and what is likely ahead. It also works like blind spot detection sensors to warn you about potential threats. While all of these components are not included in every model of car, they provide a superior experience for those who have access to and make use of them.

Surrounding these core elements is governance. Consider **governance** to be the steering mechanism that makes sure everything moves together in the right direction, as intended. This capability requires process, policies and documentation, but also executive support, corporate culture and other components that make cybersecurity a unified, repeatable and efficient capability. Governance also includes risk management — the processes a company uses to understand the threats it faces and calibrate its defenses in a way that aligns with its risk tolerance. This is a key function for board members to weigh in on.

Finally, CrowdStrike acknowledges that a car built without a suspension system is going to result in a bumpy ride and likely will detract from the overall driving experience. Similarly, an effective cybersecurity model must be supported by a strong **security foundation**. An organization's security foundation includes areas such as asset management, patching, management of end-of-life systems and other areas that make managing and securing the network easier, while simultaneously making the job of a sophisticated attacker more difficult.

Board members often ask whether they have the right security team in place. Rather than focusing on the team, CrowdStrike recommends that board members focus on these functional areas to assess the maturity level of your organization's cybersecurity. Doing so will help define the size and makeup of the appropriate team, as well as the processes and tools it needs to succeed. Approaching this in a proactive manner allows an organization to identify gaps and mitigate them, before it makes international headlines as the victim of a breach.

CrowdStrike also provides organizations with guidance about the maturity level an organization should seek, as well as how it compares to peers, across the six cybersecurity capabilities mentioned above. This comparative assessment offers another data point for the executive team and the board to consider. They should also discuss whether it's enough to be on par with one's peers. "Keeping up with the Joneses" is often not enough to keep up with threat actors.

The final point on this topic is that for those organizations with a well-known name and global presence, it's important not to define your peers as only those of a similar size within your industry. It may be equally important to consider how others in your tier are assessing their cybersecurity. If you're on the board of a Fortune 100 company, for example, consider what your peers on that list are doing and determine if there is room for you to grow accordingly.

Threat Detection Framework

In relation to the cybersecurity maturity assessment described above, board members can benefit from measuring what the organization's security team wants, in order to perform its job, against what it currently has. For instance, the head of security may identify that an endpoint protection tool will provide his team with greater prevention, detection and response capabilities, but perhaps this tool was not funded during the prior year's budget discussions. The board would benefit from knowing what gaps exist as a result of this budget-saving decision.

CrowdStrike Services uses a more direct means to achieve this awareness of gaps, through its threat detection framework. Organizations are asked to identify all of the data points they would find useful as part of proactive hunting and detection activities, as well as during an incident response. These data points are then mapped to the in-house tools and systems that provide the corresponding information. Where gaps exist, it is then possible to identify where that data or capability can be gained, either internally or through an additional toolset.

What you're left with is a picture of what information you have and what information is lacking, given your current cybersecurity capabilities. The appropriate next step after identifying the gaps is to attach a risk and cost to each. Understanding what risk will be left unaddressed if the gap is not filled, and how much it would cost the organization to close the gap, allows for a qualitative approach to risk reduction. Ultimately, most organizations will find it impossible to purchase everything on their wish lists, but the residual risk can often be addressed through other means, such as having a third party on retainer or establishing the ability to scale log retention during a suspected cyberattack.

As a board member, you want to know what this risk profile looks like — not just during a breach, but especially prior to one. Armed with this information, you can provide your organization with more specific and effective advice on how to address its current cybersecurity posture.

Next Steps in Assessing Cybersecurity Risk

"The best organizations in the world strive to detect an intrusion in under one minute on average, investigate it in under 10 minutes, and eject the adversary in under an hour. These metrics are critical for boards of directors and CEOs to track in order to measure the effectiveness of their cyber programs."

CrowdStrike Board Member

This document is intended to provide a crash course in understanding cybersecurity from a board perspective. While not altogether different from advising on other high risk areas, board members must remember that on the other side of every cyberattack is another human. This human factor is a distinguishing feature of cybersecurity incidents, and it drives the importance of developing good proactive and responsive awareness of the threats facing your organization.

The appendices that follow offer questions and considerations for board members to address with their constituents in relation to cybersecurity and incident response. Additionally, they include advice on how, as potential targets, board members should secure themselves. These guides are not comprehensive, but do outline some of the most important considerations a board member should understand to be effective advisors and leaders regarding cybersecurity.

Appendix A –

Proactive Cybersecurity Questions and Answers

Question to Ask	Positive Response
What are our biggest threats?	This should lead to a discussion around high-value assets/targets, adversary motives and impact to various types of risk (financial, reputational, operational, compliance, etc.).
What are we doing to defend against these threats?	The team should offer a view into corporate cybersecurity detection, prevention and response capabilities. These capabilities should be tailored to the threats garnered from strategic threat intelligence and compared to the risks associated with high-value asset/target information.
What are our most glaring, unmitigated or high-impact vulnerabilities?	This should elicit discussion of the internal gaps, known risk exceptions, etc., as well as a discussion of the compensating controls to address these vulnerabilities.
Where we have gaps, what is the potential impact?	The team should explain how impacts are assigned to vulnerabilities as they relate to various types of risks. Depending on the level of potential impact, the organization should revisit higher impact vulnerabilities more frequently to determine if they can be mitigated or reduced.
Would we know if we were breached?	A discussion of detective controls and the ability to monitor and alert in real time should result, along with a discussion of proactive "hunting" to look for evidence of attacker activity — even in the absence of a security alert.
Do we have an incident response (IR) plan?	The best answer would be, "Yes, and it's updated regularly to reflect the latest changes to our threat landscape and organization." Ideally the plan should address the roles and responsibilities of responders across the enterprise, not just within the IT security team.
Have we exercised the IR plan?	The answer should be, "Yes, through tabletop exercises, live fire exercises, crisis response exercises, adversary emulation exercises, etc."
Do we have retainers in place with outside counsel, crisis communications and cyber forensics firms?	Ideal answer: Yes, along with stated vendors and retainer details (start/end date, hours balance, rate, etc.).

Question to Ask	Positive Response
Do we have cyber insurance?	Yes, along with details of what is covered and who owns the responsibility for managing and updating the policy. Note that the absence of cyber insurance is not necessarily problematic, provided it is the result of a conscious decision based on an assessment of the coverage available, and in alignment with other risk management strategies.
Have we validated that we meet all the requirements under the insurance policy?	Yes, along with details of how these requirements are being met. Where applicable, these requirements should be baked into documented processes and procedures.
Have we identified our critical assets or "crown jewels"?	Yes, along with presenting a critical assets list and explaining the criteria for determining what belongs on that list.
Do we have a data classification plan?	Yes, the plan should include different levels of security based on the classification of data. For instance, sensitive data should have higher security (encryption, multi-factor authentication, etc.) than public data.
How are we protecting our executives and other individuals in leadership roles?	This should lead to a discussion of physical security for organization leaders, as well as additional IT controls or training applied to these individuals (application whitelisting leveraged on machines, multiple devices for performing different tasks, multiple user accounts, etc.). Other security steps that individuals should consider are defined in Appendix C.
Is cybersecurity integrated with physical security?	Yes, depending on the organization. This could be formalized through a "fusion center," or there may be informal relationships and information sharing processes — the more formalized, the better.
Do we leverage outside vendors for additional security support such as a managed security service provider (MSSP)?	This will depend on whether the internal team has the resources to provide these support functions, including monitoring, alerting, triaging and possibly, remediation.
What sources of threat intelligence do we have access to?	At the very least, the organization should be consuming freely available "open source" intelligence. For more mature organizations, the expectation is that paid intelligence subscriptions are in place that provide more detailed intelligence that is of greater benefit to the organization itself, both tactically and strategically. For organizations in certain sectors, formal information sharing and analysis centers (ISACs) can also provide sector-specific information about threats.
Do we leverage tactical intelligence to improve our defenses?	Yes, we apply "known bad" indicators to our detection and prevention tools. We also use threat intelligence to perform proactive "hunting," where we look for evidence of certain potentially malicious tactics and operations within our environment.

Question to Ask	Positive Response
Do we have a robust, forward-leaning strategy to incorporate threat intelligence into our security approach?	Yes, we review the current trends and specifically those likely to affect our organization on a periodic basis (monthly or quarterly), and we modify our security initiatives appropriately to address the largest risks.
Do we maintain a cyber roadmap?	Yes. The cyber roadmap should incorporate initiatives across a one- to two-year period, at a minimum, and include a prioritization based on risk, impact, difficulty, cost and other factors. The roadmap should address people, process and technology components.
Do we have an IR policy or IR playbooks?	Yes, the IR Policy defines the governing structure for the organization, granting the authority to declare and respond to an incident to certain individuals. IR playbooks are more tactical documents that can be used by groups within the organization to perform step-by-step decision-making. Typical groups assigned playbooks include IT, communications, legal, marketing, regulatory and other business functions.
Do we have pre-established communications templates that are relevant to cybersecurity specifically?	Yes. The templates should be broad enough to allow for the vast array of cybersecurity attacks, but also take into account the unique dynamics of a cyber event that is still evolving, where all of the details are likely not known (even at the end of the investigation, in some cases) and where you may not know the full impact until months later. Typically, these communications include, "The investigation is ongoing."
What key performance indicators (KPIs) are we tracking related to cybersecurity?	Possible KPIs may include operational metrics such as: alerts generated; events identified; blocked events; incidents declared; duration of incidents; impact of incidents; cost per incident; unpatched vulnerabilities; EOL systems; security technology saturation; mean time to detection; mean time to containment; mean time to remediation; and more. Additional strategic KPIs may relate to things such as: what percentage of IT spend is allocated to cybersecurity; overall cybersecurity maturity level and trend; duration of high-risk security exceptions; how we compare to our peers; whether we are compliant with regulatory requirements; any known supply chain risks, etc.
Do we have a plan in place for recovering from a destructive attack?	Organizations should treat destructive attacks with a dual focus on cybersecurity and business continuity. Similar consideration should be given to ransomware-style attacks. Testing these plans through exercises and simulations is a good practice.

Question to Ask	Positive Response
Do we maintain offline backups?	Yes, at least for critical systems and data, based on RTO/RPO. Understand the length of time backups are available as well — most organizations will want at least a few weeks' worth of backups for important systems. Also, have a discussion on the time required to restore from backup. Tape archives may take days or weeks to recover fully. Also, take into consideration the location of the backups.
To whom does the chief information security officer (CISO) report?	Typically, it's not a good idea to have the CISO report to the chief information officer (CIO). There could be a conflict of interest because the CIO is primarily concerned with business uptime, while the CISO is concerned with security, which often has a negative impact on business uptime and productivity. Good options include having the CISO report to the chief financial officer (CFO), head of legal, or (for certain organizations) the chief executive officer (CEO).
What is our patching strategy?	Critical and high-priority patches should be applied as soon as possible after any necessary testing. The patching strategy is based on the severity level of the vulnerability. Zero-day exploits are patched as they arise, outside of typical patching windows. Additionally, organizations should have different approaches for patching operating systems (e.g., Windows) and third-party applications (e.g., Adobe Acrobat), while recognizing that both are important.
Do we have end-of-life (EOL) systems in our environment, and how are we planning to manage upcoming EOL system upgrades?	If yes, there should be a plan to upgrade those systems. If upgrades are not possible for business reasons, then significant mitigating and compensating controls should be in place to address the residual risk, as these systems typically no longer get vendor-issued patches and updates.
Do we have a flat network or are network segments well-defined?	A positive response would include a discussion about internal firewalls or virtual local area networks (VLANs) that segment the network internally and provide appropriate connectivity based on the location of the system and/or the user's privileges. A flat network means that someone can move anywhere in the environment if granted the appropriate user permissions. Network segments define logical separations between different areas of the environment to prevent unauthorized access to sensitive data or content not required to fulfill daily job tasks. In addition, network segments can be used as a threat containment control for environments in hostile or untrusted geographies.
Are any segments of the environment less secure than others?	Where possible, additional security controls should be in place for high-risk network segments. This could include jump boxes to access those networks, separate credentials, multi-factor authentication or other controls.

Question to Ask	Positive Response
Do we have endpoint visibility across the network for prevention, detection and response?	The level of saturation should be high. Any gaps should have mitigating controls in place. A positive response should also include some examples of the types of visibility enabled by the security product.
Do we participate in an ISAC and/or maintain relationships with local and federal law enforcement?	Depending on the industry, the ISAC may be of great or little benefit. Establishing relationships with industry peers and the intel community more broadly would provide a good sounding board for discussing security trends and identifying attack vectors.
What proactive assessments have been conducted over the past year? Were the key findings and recommendations addressed?	A positive answer would include any or all of the following assessments, and the key findings, outcomes, and recommended implementations or locations on the roadmap: penetration testing assessment; tabletop exercise; wargame; compromise assessment; cybersecurity maturity assessment; incident response documentation development or assessment; and detailed cybersecurity roadmap development or assessment.

Appendix B –

Incident Response Questions for the Board to Consider

Initial Questions

- Has the incident been contained?
- Who is in charge? Who is the ultimate decision-maker?
- Have we established privilege? If so, through outside counsel or inside counsel?
- Have we determined the impact?
- Is there a need to involve third-party vendors, such as a forensics firm or public relations agency?
- Do we have the resources required to maintain day-to-day operations and investigate the incident?
- What are our breach notification requirements to customers, regulators, etc.?
- What is our deadline for meeting breach notification requirements and what time did that clock start?
- Do we know when and how to notify our insurance provider?
- What have we communicated internally and externally?
- What is the impact to the business, our shareholders and our employees?
- Have we established a war room?
- What is the cadence for updates?

During the Incident Response Efforts

Incident Scoping

- Have we determined the root cause/initial point of infection?
- Do we have endpoint visibility across the environment to know where the attacker is and when he moves?
- Is the attacker still active in our environment?
- Has legal reviewed file systems of compromised machines for protected health information (PHI), personally identifiable information (PII) or other controlled data types?
- Are we receiving the following data points regularly?
  - Are there any key updates to the attack timeline?
  - Has there been any change to the number of systems compromised or accessed?
  - What is the importance of these systems?
  - Has there been any change to the number of accounts compromised?
  - What is the level of access of these accounts?
  - Are there any new systems that have been collected for analysis?
  - What is the status of current systems undergoing forensic analysis?
  - What additional forensic tools or suites have we deployed during the investigation?

Communications

- Is there any indication that email, voice over IP (VOIP) or other internal communications are compromised?
- Are communications being conducted out-of-band?
- Who has been informed of the incident to date?
- Have you considered reaching out to your peers or ISAC organizations?
- Have you considered reaching out to law enforcement?
- What information are you expecting to get back from these groups?
- If the breach is public, have we advised our employees on how to respond to inquiries?
- Have we prepared a holding statement? What other public relations efforts do we anticipate?

Remediation

- What are we doing to monitor and then remove the attacker?
- Do we have enough information to begin remediating? If so, what are our proposed remediation steps?
- What is the investment required to remediate the short-term risk?

Attribution

- Have we determined attribution?
- Is there any indication that an insider could be involved?
- Will we conduct any internal interviews of employees?
- What are the possible objectives of the attacker?
  - Theft of intellectual property (IP)?
  - Theft of PII or PHI?
  - Financial motivation (e.g., ransomware, payment card theft)?
  - Destruction or disruption (e.g., distributed denial of service (DDoS), destructive malware)?

Additional Question by Attack Type

Espionage (IP Theft)

- What are the implications of the information that was taken?
- How could an adversary use the IP?
- How long would it take a competitor to replicate our product/process contained within the IP?
- What is the likelihood that the attacker would publicize the information? What would the impact of that be?
- Can you measure the potential loss in financial terms? In reputational loss?
- Should state or federal authorities be notified of the IP taken? Could the IP have a national security impact?

Criminal (PII Theft/Credit Card or Other Financial Theft)

- Have we contacted a payment card industry (PCI) forensic investigator (PFI)?
- Have we contacted the card brands?
- Do we have processes in place to increase our preparedness to deal with the number of inquiries to our website and support number?
- Are we offering credit monitoring?
- Are we doing anything additional to help our impacted customers?

Hacktivist/Ransomware/Destructive Malware/DDoS

- Do we have backups of the impacted data? How recent are they?
- How many systems were impacted?
- Have you incorporated the crisis management and business continuity process?
- If ransomware, what is our process to determine whether to pay the ransom?
- Do we know anything about the

attacker that would lead us to believe he would follow through on returning our data?

- What is the financial or oher impact (e.g., customer inconvenience or health and safety) if we can't restore systems and data?
- If DDoS, do we have DDoS mitigation vendors to offload the increased traffic?

After-Incident Containment

- How can we confirm that we have eradicated the adversary from the environment?
- What is our plan to restore the organization to business as usual (BAU)?
- Can we rely on the systems that were accessed by the adversary?
- Are there any implications for audit or regulatory filings?
- Do we need to perform manual reconciliations of SOX impacted systems that were accessed?
- What is the investment required to secure the environment against all cyberthreats in the long term?
- How did our response compare to others?
- Was the company negligent in its ability to protect our data?
- What could we have done differently or better?
- Do we need to increase or change our insurance coverage?

Appendix C –

Securing the Individual — A Guide for High-Value Individuals (HVIs)

This guide is intended to provide suggestions on how to protect employees within an organization who are considered HVIs. This could include members of the board and the executive team, as well as individuals with access to highly sensitive information, such as research and development or legal resources.

The guide includes steps that an organization's IT security team can take to monitor and enhance the security around the HVI, as well as guidance for the individual. As such, parts of this guide may be useful to any individual interested in cybersecurity best practices.

General Best Practice

Individuals should consider the following tips as part of their day-to-day security due diligence.

Personal Security

- Understand that you are a target and act accordingly. Stay alert and aware — when something seems off, trust your instincts.
- When in public, be aware of where you are and who may be watching your screen or listening to your conversations. Avoid doing sensitive work in public places.
- Monitor your credit scores regularly with proactive alerts for suspicious activity.
- Do not use corporate identifying logos or names that may draw attention on laptop bags or devices.

Email Security

- Don't click on links in email. Manually navigate to the site location where possible.
- Don't open email attachments without validating that the sender is the person you suspect it to be and that you are expecting the file.
- When possible, make sure the email applications on your devices connect through a virtual private network (VPN).
- Send emails encrypted, when possible.

Internet Security

- Don't connect to public WiFi. Avoid using hotel WiFi, when possible.

Instead, tether to your phone and use it as a hotspot.

- Leverage a paid VPN service to add a second layer of security and anonymity, using full-tunnel (not split-tunnel) VPN. The VPN should connect to servers in your home country.

Online Account Security

- Don't accept social media requests from individuals unless you know them personally or can confirm they are legitimate based on mutual connections and other supporting data points.
- Leverage multi-factor authentication for accessing corporate and personal accounts, websites and systems, where possible.

Password Security

- Use strong passwords/passphrases that are unique for each system/website.
- Use a password vault to ensure passwords are robust enough to be effective.
- Protect your password vault with multi-factor authentication.

Device Security

- Ensure all programs and operating systems are up to date with the latest upgrades and patches.
- Ensure corporate and personal devices are encrypted.
- Keep laptops turned off when not in use — not asleep, turned off.
- Keep mobile phones and tablets locked when not in use. Set them to lock after a couple of minutes of idle time.
- Keep mobile devices on your person when traveling.
- Only install applications from a trusted source. For Android devices, ensure the Google Play Store is updated to the latest version. (With Google Play version 11 and beyond, Google Play Protect will be installed and enabled by default.) For iOS devices, the App Store is much more robust due to the closed nature of the iOS code. So while the App Store has allowed malicious apps to be uploaded before, the chances are slim.
    - In any case, do not update applications via public WiFi networks on your mobile devices or laptops. Actors often use public WiFi networks to compromise high-value targets.
- Use host-based firewalls on machines, where possible.
- Do not plug unknown USB devices into your laptops.
- Do not plug into USB charging ports in public locations, or plug into other unknown devices or ports.
- Use a mobile device management solution that allows for encryption, remote wiping capabilities and preventing device rooting. For your personal devices, activate the "find my phone" feature.
- Back up data often to encrypted devices and secure backup hardware in a safe.
- Investigate the security provided by non-password locking mechanisms such as biometrics (face, fingerprint, etc.) or numbers.

Additional Travel Considerations

When individuals are traveling, the following considerations can provide enhanced prevention, detection and response capabilities. These are even more important when considering travel to potentially hostile environments.

Before the Visit

- Where feasible, bring “burner” phones and laptops rather than normal day-to-day devices.
- Ensure devices are fully patched, on the latest software versions and protected with appropriate endpoint security tools (e.g., mobile device management (MDM), endpoint protection).
- Enhance security prevention controls, including USB restrictions, hard drive encryption, etc.
- Remove unnecessary data from the system.
- Back up the contents of the device.
- Enable biometric or smartcard access to laptops, where possible.
- Take high-resolution images of the hardware to verify starting point of screws and other items to allow for comparison after trip.
- Weigh laptops and mobile devices.
- Use tamper-proof tape or epoxy to secure device from being opened without knowledge.
- Request temporary user accounts that only provide access to the data you need while traveling.

During the Visit

- Monitor devices for unknown applications and systems.
- Leverage corporate security or SOC (Security Operation Center) resources to proactively monitor for any suspicious alerts associated with the traveling individual’s devices, and treat them as a high priority.
- Connect to the Internet and resources over VPN only; select a VPN that allows you to directly connect to servers in your home country.
- Freeze credit card accounts except for one or two you plan to use.
- Use cable locks to secure devices.
- Shorten screensaver and device lock timeout periods.
- For high-risk locations, consider that even hotel safes may not offer full security and keep devices with you.
- Do not accept USB devices from any source.
- Only use power outlets for charging mobile devices, not charging stations.

After the Visit

- Compare hardware to high resolution images taken before the trip.
- Weigh devices again and compare to pre-trip weights.
- Change credentials for logging into devices and sensitive accounts.
- Where feasible, wipe devices to eliminate any applications or processes that were added during visit.
- Change any passwords to accounts accessed while traveling.
- Restore devices from a backup taken prior to trip, if necessary.

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 100 billion security events a day from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more:
https://www.crowdstrike.com/

About CrowdStrike Services

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging CrowdStrike's world-class threat intelligence and next-generation endpoint protection platform, the CrowdStrike incident response (IR) team helps customers around the world identify, track and block attackers in near real time. This unique approach allows CrowdStrike to stop unauthorized access faster, so customers can resume normal operations sooner. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately prevent damage from cyberattacks.

Learn more:
www.crowdstrike.com/services/

CROWDSTRIKE