Are We Safe?

A CEO'S GUIDE TO ADDRESSING CYBERSECURITY CONCERNS

Table of Contents

Cybersecurity Questions that All CEOs Need to Ask

The best business decisions are often made based on senior leadership's confidence in facts, figures and calculations made by appropriate parties within the organization. Relying on gut instinct—or worse, potentially false or incomplete information—is a dangerous road to travel, especially in cybersecurity.

Whereas a gut instinct may work in marketing, sales, or other facets of the business, the planning, implementation, and verification of security operations require facts to be complete and accurate. You need to have all the answers to every possible question at any time.

CompTIA's Cybersecurity Advisory Council has developed a series of questions to ask within your organization to ensure that you have a complete security picture in order to make the best decisions for the company.

Note: It's important that the person/people answering the questions recognize that they are obligated to share any and all pertinent information germane to the larger decisions being made, whether a direct request was made or not.

For each of the questions below, keep in mind that responses should also address the following questions/criteria as a baseline:

–››› Are you sure?

Cybersecurity expectations should be measured against the reality of implementation of processes, procedures, education, and verification. False assumptions or beliefs about security conditions are often found after a major security incident. These inaccurate understandings can lead to security gaps and unmitigated risks that are later found to be a potential or even predominant cause of a breach.

–››› Why are you sure?

Refrain from basing a business decision after being told that "all is good" without supporting evidence from responsible parties. Request or even require independent testing based on the outcome expected, then review those results to ensure a high level of compliance and confidence.

1 Do we keep a live inventory of assets?

In other words, do we know what needs to be protected (i.e. hardware, software licenses, IP, and other sensitive data)?

Maintaining—and continually updating—an accurate inventory of both physical and virtual assets, including all devices, licenses, and policies is critical to help determine your cyber posture and vulnerabilities. Here's a detailed look at several categories of assets:

Hardware and Software

You cannot defend assets if you are unaware of their existence, purpose, location, and status information such as configuration, age, and version. Cyber defense requires attention to details such as device type, model, operating systems, software, and firmware versions, how they are used, etc. If you ask for your company's asset inventory and get less-than-confident responses, assume you are at risk. This may sound flippant, but the reality is that even when you know what you are defending, i.e., location, condition, etc., it is still a challenge to secure. Also, you may find a device sitting in a closet, sight-unseen for months. Once it's turned on, it could be way behind on security updates, out of support, or even compromised.

Accurate inventory helps you keep up to date with accurate licensing requirements, resource allocations such as power, data, internetworking and internet throughput, physical storage, insurance coverages and even staffing and service provider qualifications and cost expectations.

Data

Your team should know what data you have, where it resides and how it is used. That's a critical part of systems design, security, and management. Having the data identified, classified, and organized also helps determine its value, who should have access, and what response is expected when illegitimate access, corruption or destruction occurs. In many cases, incident responses expose this as a glaring gap in an IT environment. Unfortunately, too many technology staffs can't accurately answer questions about where a company's data resides, who has access and even whether it is backed up properly.

Policies

Policies are a critical starting point in any risk management program, but a few important factors should be considered from the executive perspective, including the development of policies, how they were chosen and supported by processes, education, and remediation. Policies can be a huge plus in managing your security posture and can lead to great improvements, but they can also be a source of significant legal peril if improperly defined or worse, not implemented and enforced.

If your policies only reside as institutional knowledge with the heads of staff, it means there are no policies. They should be shared with and understood by employees, managers, disinterested parties, auditors, and others with an interest such as customers, partners, service providers, etc.

FOLLOW-UP QUESTIONS

- How were our polices determined?
- Were they defined specifically for our company?
- Are they simple and easy to follow?
- Do our employees understand them?
- Are we testing for behaviors?
- Do we have a mechanism for reeducation and administrative correction?
- Can our policies be audited?

2 Are my employees properly educated about cybersecurity threats?

How do we measure their knowledge/preparedness?

It's not enough to train employees by giving them information and then testing for what they remember. It's more important to show them why they need to understand the information, the ramifications for failing to act appropriately, and to randomly test them to see their responses when faced with a decision that could lead to a successful attack.

Random testing alone leads to more cautious behavior and reduction in careless or reckless actions. Testing must be sneaky and as realistic as possible without warning. Also, make it randomized so targets don't expect it or become complacent.

Some may criticize random testing as potentially embarrassing to those who fail, but embarrassment from failing a test on a job is far better than the loss of that job and potentially many more due to failing a real-world incident. Cyber simulations can cause a "fight or flight" response and muscle memory that later helps recognize a potentially bad situation and appropriate reaction.

FOLLOW-UP QUESTIONS

- How often are my employees educated about cybersecurity threats?
    - Are you sure?
    - Have they been tested?

3 Does our cybersecurity strategy address business risk? How?

It's critical to know how technology is accessed, leveraged, and the impacts of an attack on that technology. Many employees don't fully understand the business impact of a major cyber incident, whether intentional or accidental, until they are in the fog of war. It is vitally important to be award of the cascading impacts of a potential incident, from a basic outage to a major disaster or full loss of systems access and control in a ransomware event. You cannot possibly build a plan or resistance and resilience without fully understanding the ramifications of not doing so.

It's important to have the ability to recover from a ransomware incident without paying a ransom. However, the ability to operate during an attack is also worth investigating. What are the minimum continuity requirements for the organization, are we prepared to meet them, and can the IT team prove it?

FOLLOW-UP QUESTIONS

- Does our cybersecurity strategy address business risk? How?
- Is there an actual risk matrix that identifies specific business risks and how they are addressed from the security perspective?
- Are the board and business unit executives informed about our cybersecurity strategy?
- Is there a regular mechanism of communication and dialogue with the most senior executives around the who, what, where, how of the organization's security strategy and better yet, posture as measured against that strategy?
- How are we protecting ourselves in case of a breach?
- Are we aligning our cybersecurity strategy with business objectives?
- Do we have the right data governance strategy to minimize cyber risk?
- How can we operate in case of ransomware attack?
    - How long does it take for us to detect, respond and recover?
- Do we have the right data governance strategy to minimize cyber risk?

4 How would you attempt to attack us, infect our systems with ransomware, steal our data, and otherwise cause us potentially severe disruption and losses?

Answers to this can be very enlightening. It is rare that technology leaders don't know of weaknesses within their environment that could be leveraged to harm the organization. They often will not share this information unless asked specifically. Asking what they know, rather than what they want to share, often leads to more open-ended and transparent answers. If you asked a narrow question designed to limit potential answers, you will get limited, less candid answers. The goal is to unlock their deep understanding and knowledge of your environment—and what keeps them up at night.

Knowing what your technology team thinks is a critical factor in understanding your risk. Are they equipped to make necessary decisions in a vacuum, or should they be made with support from higher-level leadership? Even CIOs may often have a more myopic view of some issues that could benefit from a wider discussion of company risk exposure and tolerance levels.

FOLLOW-UP QUESTION

- What are the top three technology-related issues that could put us out of business today?

5 If we were hit by a major attack, how confident are you that we could recover quickly?

Many organizations do not have a plan for recovering from a major attack quickly. Key issues such as reducing downtime, preventing, or minimizing revenue loss, addressing customers' experiences during a recovery, and minimizing recovery costs must be addressed before an incident occurs. The absence of such a plan could create chaos while trying to recover systems and data and critical systems may not be available in a reasonable time as required by the business. Furthermore, it is not enough to simply have a plan. Environments are constantly changing, so organizations must frequently review recovery plans, prepare for a potential attack by testing those plans, and adjust as needed.

Ask for evidence of the following:

Incident Response Plans

Response plans should include the latest test results and adjustments made since the last test. An incident response plan must have an owner who is accountable to the C-level suite. The purpose of the plan is to identify, communicate and document all the key areas of business that need to be covered in case of an attack and then communicate with the C-level suite to secure the funding to implement the plan. Information technology is a key component of this plan. However, marketing, operations, customer service and sales also might have roles. Once the plan is approved and implemented, its execution can be tested and results reviewed regularly. Are there any adjustments that need to be made because of the changes in the environment, personnel, or reporting structure?

Disaster Recovery Plans

Include latest test results and adjustments. Disaster recovery (DR) refers to the ability to recover from a catastrophic failure. In the past, it was typically systems related, but ransomware has recently been added to the list. Business continuity (BC) refers to the ability to continue operations even through a catastrophic incident. For example, having a secondary duplicate site that will take over as needed. Organizations must test their DR/BC environments on a regular basis and be able to present the documented test results.

Business Continuity Plans

Assume a worst-case ransomware or other broadly destructive/disruptive incident. How would you continue operations? Are there offsite backups that can be restored immediately or secondary sites that can be turned on? How long does it take to restore backups or turn on the secondary sites?

Insider Protections

Ransomware and other major attacks no longer come exclusively from the outside of the organization. Increasingly, an unaware internal user might unintentionally introduce malware in the organization that can result in a major attack. There are several tools that can help organizations identify insider attacks and provide protection in real time. How is your organization protecting itself from these attacks? What tools have been deployed and how are they monitored? Does the C-level suite have visibility into measures taken for insider attacks?

If your policies only reside as institutional knowledge with the heads of staff, it means there are no policies. They should be shared with and understood by employees, managers, disinterested parties, auditors, and others with an interest such as customers, partners, service providers, etc.

FOLLOW-UP QUESTIONS

- Can our IT department demonstrate the right reporting and systems?
- What are you monitoring and measuring to make sure we are protected?

6 What preventative measures have you implemented already to protect our company?

In order to properly evaluate an organization's cybersecurity program, it's incredibly important for business leadership to understand the current systems in place. In particular, the tools deployed to prevent or reduce threats potentially impacting the organization. These systems should be verified, documented, and tested frequently with detailed reporting output.

FOLLOW-UP QUESTIONS

- How do you know our measures are effective, i.e., can you demonstrate how you are following best practices?
- Has anyone (outside of the organization) reviewed and verified that we have sufficient preventative measures in place?

7 How do you measure and manage our cybersecurity program?

In order to maintain an ever-evolving, ever-maturing security program, it's paramount that your organization leverage clear objectives and metrics wherever possible. The beauty of a cybersecurity program is that all initiatives ultimately lead back to tangible risks, which allows for your organization to establish a quantifiable action to address said risk.

These quantified metrics can be something simple, like a calculation of how many of your IT controls passed vs. failed during an assessment, or how many new hires had a background check and how many did not.

But one of the most exciting elements of building an evolving security program is that as your program matures, your metrics become more advanced. You begin to establish Key Risk Indicators (KRI) and Key Performance Indicators (KPI) that can tie back to monetary values. For example, you might scope the likelihood and impact of a ransomware attack to your organization once every four years and calculate that the expected impact of the attack would be $500,000. Divided across four years, you've successfully just calculated an annualized expected cost of $125,000 for your organization that can now be budgeted for.

FOLLOW-UP QUESTIONS

- What KPIs do you use?
- Do you have leading or lagging indicators of our organization's cyber health?

8 How do you determine the appropriate budget for technology risk management?

As cyber threats continue to increase, aligning appropriate budget with technology risk management should be a top priority. Cybersecurity spend is like having insurance. It may be hard to measure, but it is required to reduce risk of revenue loss, customer information, intellectual property, company downtime, and reputation.

No matter how many technology companies you have incorporated or how good you believe your cyber hygiene is, there's always room for improvement. Most CISOs and companies don't have an infinite budget, but cybersecurity spend is an essential cost of doing business: "an ounce of prevention is better than a pound of cure."

Experts advise that 10% to 15% of an organization's IT budget be allocated for protection against data breaches and cybersecurity attacks. The higher your current risk, the larger the investment needed. Estimate your value of your company's net worth, including risk of down time, should a cyberattack happen, to determine the value of business loss.

FOLLOW-UP QUESTIONS

- What percentage of our IT budget is allocated for cybersecurity?
- How do we determine that percentage each year?
- Do we calculate potential business loss caused by an attack?

9 What does the threat outlook mean to your resilience strategy?

Companies failed to anticipate the impact posed by a global pandemic, sacrificing security process in the interest of business continuity and availability. Workers moved to unmanaged home networks and IT and security teams lost visibility to what devices had access to high-value data, applications, and the health of connected devices.

The outcome was not unexpected: 2020 was the worst year on record for cyber-attacks and 2021 has been more of the same. Many organizations did not survive, primarily SMBs that lacked resources to adapt their security posture.

But the trend is not completely new. Organization attack surfaces have continually increased as data, infrastructure and applications shift to the center of business and society. Our digital economy has become fragile and faces an inflection point of how we adapt and survive a potential if not already forming cyber pandemic.

It's critical that businesses respond appropriately and quickly to address the continually changing threat landscape.

FOLLOW-UP QUESTIONS

- What is driving our resilience strategy?
- What are we doing specifically to respond to address evolving risks?

10 How do you find, recruit, and retain the best cyber talent available, or find the best combination of managed services and cyber talent in a competitive market?

To attract the best cyber talent, start with a resource requirements matrix that includes current requirements and planned resource needs for the next six to 12 months. The matrix should include key decision points such as cost of resources (hourly or subscription), preferred channel (contractor, FTE, managed service provider), and any regulatory constraints or overhead. Note that the matrix will most likely include headcount and resources across multiple areas and lines of business within the organization.

Use the matrix above to assess the current talent pool and determine overlaps and gaps in staffing. Build out a plan to address the gaps and eliminate any overlaps. You may find that overlapped roles can help fill in gaps.

It's important to identify required qualifications for all cybersecurity personnel. The qualifications should be based on the role and responsibilities associated with and required for specific roles. A data center or NOC/SOC manager may need to be on premise and have physical security expertise to ensure the center is properly secured, but a threat hunter may be able to work from anywhere and have no physical security expertise. Role qualifications should be revisited at least once per year to ensure personnel are current with modern certifications and critical learning paths.

Don't forget to have the information security manager work with HR to create the right requirements documents and hire the right candidates. After defining the requirements for the role including educational background, work experience, certifications, and degrees, the manager should communicate those clearly to HR in the job description. Additionally, it should be clear which requirements are absolute and which may be optional. Job descriptions should be written realistically. Don't have the philosophy of asking for 110% of skills required and then hiring a candidate with 80% of the skills listed. This approach often backfires and means fewer qualified candidates apply which is why it's so important for the manager to work with HR on realistic and fillable descriptions. Descriptions should also use gender neutral wording.

FOLLOW-UP QUESTIONS

- Do we know which resources are necessary vs. optional?
- Have we developed qualifications for all cyber personnel?
- What's our biggest challenge in hiring cyber talent?

11 What types of risks are currently threatening our network/systems?

How do we know we have full visibility of those threats? Do we have visibility across all systems or just critical infrastructure? What steps (if any) have we done to reduce them?

Managing risk and ensuring continuity takes an organization level commitment to a culture of resilience. Many areas for improvement are operational: a lack of proper planning and preparation for adversity, siloed teams without insight into systemwide operational interdependencies or aligned to business risk, and the transformation of risk management to an operational activity. Resilience requires bringing the areas of risk management, business continuity, and IT/Dev/Sec ops together to produce a secure by design operational process supporting mission critical functions.

Of course, each business is different, and not all data, infrastructure, applications, systems, and source code are equally mission-critical or valuable to that organization. On the other hand, access to some seemingly less critical systems can serve as an entry point for an attacker as everything is connected and one human or technical error can lead to a crippling attack.

FOLLOW-UP QUESTIONS

- Are we monitoring for threats across the enterprise specific to our risk?
- Does our monitoring include non-persistent connection (e.g., BYOD, remote workers, IoT)?
- What is our visibility to attack life cycle? What do you see? Where? When?
- How do we manage our supply chain threats?
- Do you know your actual attack surface?

About the Cybersecurity Advisory Council

The CompTIA Cybersecurity Advisory Council brings together thought leaders and innovators from a multitude of disciplines, working together to educate technology solution providers on the latest and greatest cybersecurity practices and protocols for business.

What We Stand For

Cybersecurity is a critical component for every business and any technology solution today, but one that requires constant vigilance, collaboration, and communication. We strive to address some of today's most pressing issues and threats, providing guidance for tech companies of all sizes.

How We're Making an Impact

The pressure from hackers and other bad actors isn't abating. Thus, it's critical for tech companies to continue their investments in both cybersecurity protocols as well as developing the next generation of resources that will be required to protect assets. The Cybersecurity Advisory Council's roster of industry experts and thought leaders offers the guidance and tools necessary to help tech businesses stay ahead of the curve.