TANIUM

Cybersecurity readiness checklist for board members

With organizations everywhere facing increased threats from ransomware, data breaches, and other types of attacks, board members may wonder where their own organizations stand when it comes to cybersecurity readiness. After all, board members have a duty to ensure their organization protects itself against cyberattacks and accidental data leaks. But most board members don't consider themselves cybersecurity experts. What questions should they ask their CIOs to assess the organization's overall cybersecurity readiness?

Here's a list of questions board members can ask CIOs and other executives to ensure the organization is making the right strategic investments in cybersecurity.

Questions for CIOs about cybersecurity readiness

Have we prioritized our objectives and our risks?

Risks are uncertainties about outcomes. Risks matter most when they pertain to the outcomes an organization cares about the most. Does the organization have a risk management practice in place that identifies its highest-level objectives?

For most organizations, those objectives will include:

- Business continuity
- Data confidentiality, integrity, and availability (data "CIA")
- Regulatory compliance

Have we identified the IT resources and processes that support our objectives?

Besides identifying its key objectives, the organization needs to identify the IT resources and processes that support those objectives. For example, if business continuity depends on an ecommerce website, which IT assets, processes and teams does that website depend on? What are the company's most valuable assets? Do they include intellectual property, financial data, physical infrastructure, or something else? Where are those assets stored, and who has access to them?

Have we identified the risks associated with each of those IT resources and processes?

Board members and the executive team need to understand what makes the IT resources, processes and teams supporting each key objective vulnerable to attack. Unpatched software? Unreliable hardware? Lack of training? Have governments or industry groups adopted new regulations that will require redesigning and redeploying software and hardware?

Have we assessed the likelihood of these risks?

If the IT organization estimates the odds of a data breach to be just 1%, that's too low to be realistic. If the odds are 80%, then the organization isn't making the right investments in cybersecurity. What is our confidence level in our cybersecurity posture, and how does that level compare to those of our peer organizations? Has the organization assessed the combined likelihood and severity of each risk, so that risks can be compared and prioritized?

Have we developed a software Bill of Materials (SBOM) for all our key applications and software services?

An SBOM is a catalog of all the software components and their versions that goes into an application or software service. By compiling SBOMs, IT organizations make it much easier to identify applications and services that are at risk when new vulnerabilities are announced, such as the Log4j vulnerability that was announced in December 2021. Has the organization begun the practice of automatically compiling SBOMs for key applications and services? What's the plan for doing so? How far along is the process now? How is this work being automated, so it's always up to date?

Do we have a real-time inventory of all our IT assets, including laptops, desktops, servers, and IoT devices?

You can't secure something if you don't know you have it. As part of its cybersecurity program, an organization needs a comprehensive inventory of all its IT assets, recognizing that this inventory changes continually. How are we compiling this inventory? How regularly is it updated? How are we determining that it really is complete and accurate?

Have you identified likely adversaries and their goals?

Identifying adversaries and their goals helps the organization focus its investments on cybersecurity. Are there specific parties, such as cybercriminal gangs, nation-states, or activists who are likely to attack us? If so, what are their goals? Are they hoping to steal information, inflict a ransomware attack and demand funds, cause mayhem, or somehow damage the organization's brand? How is this knowledge shaping our cybersecurity strategy?

How are we prioritizing our spending on risk?

Trying to eliminate all risk would be cost-prohibitive. How are we prioritizing our investments? Who is involved in making decisions about spending? How often are those decisions reviewed and, if necessary, adjusted?

What plans do we have in place to mitigate risks if attacks or other undesirable outcomes occur?

Do we have teams in place ready to respond to our most serious risks? Are communication channels in place? Do team members have the tools they need to act quickly and effectively? Have teams practiced responses to attacks to ensure that people, processes and tools are ready for action?

Get Risk Assessment

Request a five-day, no-cost risk assessment to get a comprehensive view of risk posture across the organization.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.