CADENCE CYBER

Questions Smart Leaders Ask About Cybersecurity

1 Does our organization have a formal information security plan in writing?

A formal Information Security Plan (ISP) is a written document that outlines an organization's policies, procedures, and guidelines for protecting its information and information systems. an ISP is critical for protecting an organization's sensitive information, complying with regulations and standards, reducing risk, enhancing business continuity, and demonstrating due diligence.programs.

2 What are our most important assets and how are we protecting them?

Complete security is not possible, nor are budgets unlimited. Leaders must **make sure the organization's most important assets are correctly identified** and are secured at the highest reasonable level.

Is your "most important digital asset" your customer data, the systems and processes that operate your company, or is it your company's intellectual property?

3 How deep is our defense? What are the layers of protection we have in place?

Effective cybersecurity is done with multiple layers of defense, procedures, policies, and risk management approaches. How are your perimeters, applications, end-points, network and data secured? Leadership should be in an advisory role when layers of defense are planned.

4 How do we know if we've bee n breached? How do we detect a breach?

The unfortunate reality for a majority of organizations, the organization discovers a brech in one of three ways:

1. An employee is greeted with a ransom note when they sit down at their workstation.
2. Business owners receive a call from the FBI or CISA to follow up on why an intelligence source has detected a breach at your company.
3. You receive an incendiary call from a customer who discovered that their personal data has been published on the dark web from doing business with your organization.

When an incident occurs, be the first to know, not the last. The officers and board are ignoring an important part of their fiduciary responsibility if it does not ensure that the organization has both protection and detection capabilities.

5 How do we respond to an incident? Who is responsible for the plan being up to date?

When an incident is detected, then what? If there isn't a plan when the incident occurs, it is too late to start formulating one.

- Who is responsible for maintaining the plan?
- What is our ransom payment policy?
- What is our communications plan?
- Who (if anyone) talks to the appropriate authorities?
- Do we have any regulatory reporting requirements?
- Who talks to customers? Suppliers?
- How do we recover?

Having a plan for incident response is crucial for effectively responding to and eventually recovering from a security breach. While it is still true that no plan survives initial contact with an adversary, organizations that lack a plan are unlikely to withstand the initial impact of a breach.

PLAN • DETECT • RESPOND
Cadence-Cyber.com
info@cadence-cyber.com
727-546-4646

CADENCE CYBER

6 Are we training our people to recognize phishing and social engineering?

Verizon's 2022 Data Breach Investigations Report:

- 25% of all data breaches involve phishing;
- 85% of data breaches involve a human element.

Terranova Security's 2022 Gone Phishing Tournament:

- 20% of all employees are likely to click on phishing email links;
- 68% of those continue to enter their credentials on a phishing website.

Nearly 14% of employees are likely to submit their password on a fraudulent phishing page. Educating employees to detect the most recent scams is critical.

7 How are we protecting ourselves and our partners from BEC?

Ransomware and breaches always make headlines (and TV shows). But according to the FBI, Business Email Compromise (BEC) actually happens far more often and costs far more money than other cyber related crimes. In 2021, there were over 20,000 BEC complaints filed with the FBI with an adjusted loss of $2.4 billion dollars, putting it at the top of the list.

Deepfake technology will drive that number much higher when an indistinguishable AI version of a CEO can call (or even Zoom) into the organization and direct payments to be made. This has already happened. Leaders need to put in comprehensive training and procedures to prevent BEC.

8 Have we evaluated our supply chain partner's security measures?

An HVAC company contracted by national retailer Target was hacked and provided a back door into Target's lucrative data. Hacker's acquired more than 40 million customer credit cards. Target was on the hook for this mishap.

Breaches don't have to be direct; cyber criminals always look for easy targets. They count moving the breach to include the target's client base. **Are you taking measures to evaluate your suppliers and customers?** Are there any potential threats from their connections?

9 Is our cybersecurity budget right?

No business can be 100% secure. We all have an organizational budget, and a portion of that budget absolutely needs to be devoted to address technical problems and protect against the vulnerabilities inherent in critical business functions. But how does that budget get set appropriately? By applying principles of risk management: assessing asset value, vulnerabilities, and likelihood of loss, organizations can make informed decisions about budget to protect those assets.

Bottom line is that cybersecurity is a specific specialty and management responsibility, not just an IT function. There are some IT professionals that are also very skilled at cybersecurity, but they should be recognized as two different professions. The executive officers and particularly the board of directors are responsible for oversight. Don't be willfully blind. Ask the right questions. Cadence Cyber operates on a fractional or virtual basis and provides the expertise needed to build a credible defense for your organization.

PLAN • DETECT • RESPOND

Cadence-Cyber.com

info@cadence-cyber.com

727-546-4646