Ten Questions to Ask Your CISO

Not sure if you're prepared for a ransomware attack? Instead of worrying, get ahead of the threat by quizzing your CISO and security team about "what if" scenarios and plans to get up and running quickly should your organization fall victim to an attack. The questions below can help you discover what safeguards are in place and where you might be falling short in deterring cyberthreats.

1

Do we have an effective vulnerability and patch management program?

Installing software patches and updating systems to eliminate vulnerabilities are the low-hanging fruit of security tasks. If your security team confirms that your company has a patch management program, then the next questions to ask are: How do we measure success, and what are the SLAs? If the security team tells you there is no patch management program or the program is too slow or ineffective, it's time to get one started.

Ideally, teams should target patch installation within days or a couple of weeks. For major releases, the target should be n-1, or at worst n-2.

2

Do we have a recovery plan in case we suffer a ransomware attack?

How will data be restored, what does the restore process look like, what will be manual, and how long it could take? If it takes several hours (or days) to restore data, there's room to improve. Consider setting up forensics retainers with outside firms that clearly define SLAs, response, and cost—before attacks happen. Discuss the potential benefits of tiered security architectures, which can help retain large amounts of data and make it available immediately. Application tiers should be well-defined so that business units know the timeline for restoring applications.

3

How often do we test how our systems would perform in the event of an attack?

Tests should produce documented results that allow the security team to confidently benchmark the time to normal operations. Create a recovery heatmap that includes which apps are tested, how frequently, and what the results are. The documentation should also focus on critical infrastructure that can be rapidly restored in an outage since other applications depend on it.

4

What is our maximum tolerable downtime?

The goal should always be zero downtime, but in the event of a ransomware attack, there will be *some* downtime. So how much can the business tolerate? And what is that decision based on?

5

Who are our existing security and recovery vendors and partners?

It's important to compile lists of cell phone numbers and email addresses for contacts inside and outside security, including forensic and recovery vendors and consultants.

6 If we are under attack, how will we communicate?

Security teams need well-defined communications plans when it's time to inform leaders about the onset of a cyberattack. If systems and email are down, you'll need up-to-date and easily accessible lists of cell phone numbers and alternate email addresses. These should include contacts within IT and security teams, senior leaders, and third-party providers, such as the retained forensics team and cyber insurance providers.

Prepare an external communications plan for working with the media, regulators, legal teams, and local offices of law enforcement authorities, such as the FBI in the United States.

7 Are we getting enough ROI from our SIEM solutions? Do we have the visibility and speed we need?

SIEM solutions come with plenty of capabilities right out of the box, but still rely on underlying storage solutions to be fast and effective. Ask your CISO to dig into SIEM capabilities and performance and consider a storage solution with built-in anomaly detection that could indicate an attack.

8 How do we make ourselves more expensive to attack than other targets?

You want to be as costly and time-consuming a target as possible for attackers, who are also running a business and looking for attack ROI. What measures are in place to make breaching your defenses arduous and expensive? What's the cost to attack you?

9 Do we have an estimated cost to recover?

The cost estimations should be part of any planning exercises that gauge the impact of an attack, like downtime. With a budget in mind, security teams and senior leaders can put budgets in place ahead of any attacks.

10 How can we work together to assess cybersecurity risks?

If the CISO and the security team work in their own siloes, cut off from senior leaders, there isn't much hope in obtaining answers to any of the above questions on a timely basis. Instead, connect with the CISO to hash out plans for regular briefings within boardrooms, so issues and emergencies get the attention of the C-suite.

Recover quickly to a clean environment

Getting back online during the forensic process is key—and the right storage provider can be the difference between days and weeks.

The Pure Storage Evergreen//One™ Cyber Recovery SLA addresses many of these recovery steps. The SLA provides next business day shipping of clean recovery array(s), 8 TiB/hour data transfer rate, and a technical services engineering team to finalize the recovery plan, plus an onsite professional services engineer from time of array arrival through replacement of infected array(s).

PS2660-01-en 08/24