10 Questions to Ask Your Security Team

Guidance for creating a better security strategy for your organization.

If you’re losing sleep over cyberattacks, it’s time to sit down with your CISO or other security team members to discuss your organization’s cybersecurity defenses. The questions below will give you action items to discover what safeguards are in place and where you might be falling short in deterring cyber threats.

1 Do we have a vulnerability and patch management program? How do we measure its effectiveness?

Installing software patches and updating systems to eliminate vulnerabilities are the low-hanging fruit of security tasks. If the security team tells you there is no patch management program or the program is too slow or ineffective, there’s no time like the present to get one started.

2 Do we have a recovery plan mapped out in case we do suffer a ransomware attack? How will we restore data?

Security teams should consider setting up forensics retainers with outside firms that clearly define SLAs, response, and cost. In addition, understand how your data will be restored, what the restore process looks like, what will be manual, and how long it could take. If it takes several hours (or days) to be restored, there’s room to improve (and Pure can help). Discuss the potential benefits of tiered security architectures and “data bunkers.”

3 What is our maximum tolerable downtime?

Ideally, there’s zero downtime, but that’s not realistic. In the event of a ransomware attack, there will be some downtime. How much can the business tolerate? If you’re in healthcare and patient data is involved, maybe the answer is one hour. If you run a seasonal imports business, maybe the maximum is longer.

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

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.

5 Who are our existing security and recovery vendors/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 hit by ransomware, how will we communicate as an organization?

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 to have up-to-date, accessible lists of cell phone numbers and alternate email addresses for contacts within IT and security teams, senior leaders, and third-party providers.

7 How can we join forces to assess cybersecurity risks?

Connect the CISO and the security team with senior leaders to hash out plans for regular briefings within boardrooms, so issues and emergencies get the attention of the C-suite.

8 Are you willing to pay a ransom—and if so, how's your bitcoin reserve?

Decide as an organization how much you're willing to pay out to attackers if it comes to that. If business leaders agree on an amount, make sure you have a bitcoin reserve available, since you don't want to be scrambling for payment in the heat of the moment.

9 Have we run tabletop exercises to role play what would happen during an event?

Tabletop exercises take security teams through different "what-if" scenarios related to cyberattacks of all kinds.

10 Do we have an estimated cost to recover? Cost of an attack?

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 motion ahead of any attacks.

purestorage.com

800.379.PURE

PURESTORAGE®