AUDITBOARD

Ransomware Prevention Checklist: 5 Steps to Prepare

AUDITBOARD

Ransomware Prevention Checklist: 5 Steps to Prepare

Several high-profile ransomware attacks, including an incident involving Colonial Pipeline, which resulted in fuel shortages on the east coast, underscore the severity of the threat and why your organization should take steps to harden its defenses. Cybersecurity Ventures predicts that by 2031, ransomware will generate losses of $265 billion per year, with an attack taking place every two seconds.

As the name suggests, a ***ransomware attack happens when cybercriminals gain control of an organization's data and deny access until they receive a ransom payment***. While every form of cyberattack can prove costly and frustrating, forcing a company to pay a ransom to access its data can be particularly infuriating. Following these five steps will help reduce the chances of a ransomware attack and mitigate the effects of a breach.

Ransomware Prevention Checklist

1. Educate employees

Ransomware attacks often occur when an employee opens an email infected with malware. Once installed the malware scans for critical data, which the criminals then encrypt and hold for ransom. ***Educating employees on the ransomware threat and what to do if they receive a suspicious email is crucial to prevent a cybersecurity breach***. A great way to do this outside of standard information security training is through phishing and social engineering simulation tests within your organization.

It is also imperative to make sure third-party vendors educate their employees on cybersecurity best practices as criminals can

> *a ransomware attack happens when cybercriminals gain control of an organization's data and deny access until they receive a ransom payment.*

exploit their weaknesses to breach your company. As part of your standard vendor review process, make sure you are understanding the lengths your vendors are taking to instill security in the overall culture of their organization.

2. Use two-factor authentication and embrace zero trust

Multi-factor authentication (MFA), which requires a user to successfully present two or more pieces of evidence to an authentication mechanism, oftentimes through a one-time password delivered via text to access a system makes it considerably more difficult for cybercriminals to breach your defenses. ***MFA coupled with zero trust security, which removes trust as a default condition for users and devices, adds yet another level of security***.

3. Keep anti-virus and malware detection software current

Make sure your organization keeps its threat detection software up to date, as it is the first line of defense in thwarting an attack. Additionally, as soon as software patches become available, assign responsibility for their installation. The longer it takes to install a software patch, the more likely criminals will exploit the weakness it is designed to address.

4. Limit data access

If every employee receives the same level of data access, any attack can provide a path to your organization's most sensitive and valuable data. ***Following access management best practices can ensure employees only receive access to data critical to performing their role***; this includes removing data access privileges related to their previous positions. If an employee leaves your organization voluntarily or is terminated, delete their data access privileges immediately.

5. Routinely backup data

When companies cannot restore data from a backup, the only option they face is to pay a ransom. ***To avoid losing control of your data, ensure that it is backed up in the cloud or external location***. Wherever your backup data resides, make sure there's robust security in place to deny unauthorized access. Additionally, prohibit the modification, deletion, or copying of backup data.

Ransomware attacks take advantage of organizational complacency. Securing critical data and preventing others from assuming control requires a multi-pronged approach. ***While investing in a robust security program will not stop every attempt, every layer of security your organization adds increases the likelihood that a cybercriminal will divert their attention to less secure targets***.

AuditBoard transforms how audit, risk, and compliance professionals manage today's dynamic risk landscape with a modern, connected platform that engages the front lines, surfaces the risks that matter, and drives better strategic decision-making.