Five Tips to Safeguard Your Business Against a Ransomware Attack

What you need to know today to protect yourself tomorrow

What is a threat?

In a ransomware attack, a hacker penetrates an organization's network and holds its data hostage until a specified ransom is paid. Hackers don't discriminate based on business size or industry — any organization that stores its data on a network is at risk

Protect your business with these five best practices:

1. **BACK UP YOUR DATA REGULARLY.**

   If a ransomware event occurs, you'll want to access your backup data quickly. As a general rule, you should back up as often as you can. But each business is different; for instance, if your data changes significantly hour-to-hour, then back up in real time

2. **SCAN FOR VIRUSES REGULARLY.**

   Scan across your entire network infrastructure, including databases. This is especially critical for organizations with multiple IT managers or locations.

3. **TRAIN YOUR EMPLOYEES.**

   Train your employees to recognize and delete phishing and malware emails without opening them. This critical step can't be the sole responsibility of the IT department —it requires a top-down, organization-wide culture of security.

4. MAINTAIN AN INCIDENT RESPONSE PLAN.

While you might be able to get your network back up and running after a ransomware attack, the hacker could get to it first. In that case, you'll have to make quick decisions: Will you pay the ransom? Will you negotiate? It pays to answer these questions in advance. In order to respond quickly and appropriately, you should take the following steps now:

- Identify key stakeholders who will play a role in your response, including:
  - Internal: Legal, HR and IT representatives, and a spokesperson
  - External: Cyber insurance broker, privacy attorneys and a cryptocurrency broker (since hackers may request payment in bitcoins)
- Plan to minimize the harm to your organization's finances and reputation.
  - Decide if you will offer credit monitoring services or establish a call center to field customer concerns.
- Retain robust cyber insurance that offers real data breach resources in addition to policy coverage. Ask your broker about their resources to help you pay a bitcoin ransom, conduct the forensics investigation and implement notification procedures.

5. KEEP LOGS TO PRESERVE EVIDENCE.

Identify the evidence you will need to preserve, and keep detailed network access logs. This will help you more easily identify the breach site, point of entry and any exposed/accessed data or intellectual property.

We're HUB

We help you prepare for the unexpected. When you partner with us, you're at the center of a vast network of experts who will help you reach your goals through risk services, claims management, and compliance guidance. With HUB, you have peace of mind that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that put you in control.

Contact a broker today at:
hubinternational.com/RansomwareTips

HUB