In the World of Ransomware Attacks, Déjà Vu Seems to be the New Normal for Employers

Insights
9.16.21

Pick the date and news publication. After a few flips of the pages (or a scroll of the mouse), you'll no doubt find an article about "ABC Company" reeling from a ransomware attack. This proliferation of cyberattacks is all too familiar and the source of sleepless nights for many employers. The COVID-19 pandemic has played a major role in the increase, as IT departments were afforded little time to strengthen networks and data security protocols once companies abruptly shifted to a remote work environment. Some reports suggest ransomware attacks have increased by as much as 800% during the pandemic. Unfortunately, cybercriminals don't disparately select their targets – very few, if any, companies are immune from their reach. Higher education institutions have even felt the brunt of ransomware attacks, with some being forced to cancel classes to limit the number of users on their network to slow the spread of malicious software. What can you do minimize your chances of being a victim – and what should you do in case you fall prey to a cyberattack?

Are Employers Just Sitting Ducks?

Absolutely not. There are numerous steps you can take to strengthen your data security protocols and stave off cybersecurity attacks. On August 23, the Cybersecurity and Infrastructure Security Agency (CISA) released a fact sheet that provides employers with recommendations on how to prevent ransomware attacks and protect sensitive and personal information from data breaches. The CISA's fact sheet builds on the agency's ransomware guidance from last year, with specific recommendations on protecting personal data. It contains tips such as developing an incident response plan, regular scans and software updates, training employees on phishing attempts, and creating an environment of "good cyber hygiene."

Here are the highlights from the CISA's latest guidance:

Preventing Ransomware Attacks

- Maintain offline, encrypted backups of data and regularly test your backups.
- Create, maintain, and exercise a basic cyber incident response plan, resiliency plan, and associated communications plan.
    - The cyber incident response plan should include response and notification procedures for ransomware incidents.

- Mitigate internet-facing vulnerabilities and misconfigurations.
  - Employ best practices for use of Remote Desktop Protocol (RDP) and other remote desktop services;
  - Conduct regular vulnerability scanning;
  - Update software; and
  - Ensure that devices are properly configured and security features are enabled.
- Reduce the risk of phishing emails by enabling stronger spam filters, and implementing a cybersecurity user awareness and training program.

Protect Sensitive and Personal Information

- Know what personal and sensitive information is stored on your network and who has access to it.
- Identify the computers or servers where sensitive personal information is stored, and ensure it is encrypted.
- Implement firewalls to protect networks and systems from malicious or unnecessary network traffic.
- Consider applying network segmentation to further protect systems storing sensitive or personal information.

What Should We Do if Our Company is The Victim of a Ransomware Attack?

If your company becomes the victim of a ransomware attack, the CISA recommends implementing your cyber incident response plan and taking the following steps:

- determine which systems were impacted and immediately isolate them;
- if affected devices cannot be removed from the network (or if the network cannot be temporarily shut down), power infected devices down to avoid further spread of the ransomware infection;
- triage impacted systems for restoration and recovery;
- engage your internal and external stakeholders;
- consider retaining a third-party incident response provider with experience in data breaches; and
- notify affected individuals and report the incident to your local FBI field office.

Companies that become victim of a ransomware attack should also hire legal counsel with data breach experience to provide advice on potential notification obligations and to ensure compliance with reporting requirements, as well as to engage appropriate vendors to assist in investigation of the incident.

Importantly, before engaging with the individual(s) responsible for the ransomware attack, take note of the October 2020 advisory opinion from the Department of Treasury's Office of Foreign Asset Controls (OFAC) indicating that companies involved in facilitating ransomware payments may encourage future ransomware payment demands and also risk violating OFAC regulations. As a result, you might face civil penalties for paying ransomware demands. If confronted with a ransomware attack, you should consider promptly contacting federal authorities for guidance, in addition to seeking legal counsel.

Conclusion

Fisher Phillips will continue to monitor any further developments in this area as they occur, so you should ensure you are subscribed to Fisher Phillips' Insight system to gather the most up-to-date information. If you have any questions regarding how cybersecurity threats could impact your organization, or best practices for addressing those threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of Fisher Phillips' Privacy and Cyber Practice Group.

Service Focus

Counseling and Advice

Privacy and Cyber