SOCIUS

Don't Forget Cyber Hygiene When Returning to the Office

During the pandemic, many employees switched to remote work – and cyberattacks surged. Now, many workers are returning to the office, but cyberattacks aren't decreasing. Ransomware and other cyber incidents remain a growing problem. As a result, cyber insurers are enforcing good cyber hygiene.

Brokers - As your clients' workplaces return to normal, make sure that old habits and outdated practices don't undermine their cybersecurity. Be sure to share the following information.

Remote Work and Cyberattacks

The switch to remote work occurred out of necessity – and it did not always go smoothly. As workers adjusted to new procedures, cybercriminals took advantage of both the confusion associated with rapidly changing processes and the technical vulnerabilities associated with home office and remote access.

The Internet Crime Complaint Center (IC3) says that criminals used phishing, spoofing, extortion, and other tactics to target victims during the pandemic. Ransomware proliferated as hackers launched phishing attacks and exploited Remote Desktop Protocol and software vulnerabilities to access systems.

One might have expected cyberattacks to lessen once workers ironed out their remote work arrangements, but this did not happen. The attacks continued in 2021: in particular, ransomware attacks increased in both frequency and severity. According to the State of Ransomware 2022 report from Sophos, 66 percent of organizations were hit with ransomware in 2021, up from 37 percent in 2020. The average ransomware payment was $812,360, up significantly from $170,000 in 2020, but only 4 percent of organizations that paid received all their data back.

The Impact on Insurance

The rise in cyberattacks has led to increased interest in cyber insurance, but it has also made insurers more wary of underwriting risky accounts. Insurers need to manage their loss ratio. If they are constantly paying massive claims, the situation simply is not sustainable.

The Q1 2022 Commercial Property/Casualty Market Report from Council of Insurance Agents & Brokers (CIAB) shows that premiums for cyber insurance increased an average of 27.5 percent the first quarter of 2022, following an increase of 34.3 percent in the fourth quarter of 2021. Although rates have been going up across the board, these increases are significantly steeper than the premium increases in other lines. The hikes have been blamed on the increase in cyber claims. Indeed, 72 percent of respondents reported an increase in claims.

© Socius Insurance 2021. All Rights Reserved.
License# 0D6077

The Importance of Understanding Your Insurance Terms

Both insurance companies and the organizations they insure have a vested interest in preventing cyberattacks. CIAB says that underwriters have been implementing stricter underwriting requirements in an attempt to mitigate losses. For example, many insurers are mandating multifactor authentication (MFA) and other cybersecurity protocols.

Failing to meet these requirements may have dire consequences. According to Insurance Journal, one cyber insurance carrier voided its cyber policy when the company allegedly mispresented its use of multifactor authentication – something the carrier discovered after a ransomware event occurred.

This should serve as a warning to anyone seeking cyber insurance: insurers take their cybersecurity requirements seriously. If the applications include incorrect information or mispresent the policyholder's cybersecurity practices, the insurer could deny future claims or void coverage retroactively.

It is important to give cyber applications the attention they deserve. Applicants should talk to their brokers and consultants before signing to ensure that they understand the questions and answer appropriately.

Returning to the Office – But Not to Poor Cyber Hygiene

Cyber insurance provides critical protection, but it is not a substitute for good cyber hygiene. Organizations need to do everything in their power to prevent cyberattacks from occurring; otherwise, they may find themselves victims of an attack only to have their insurance claim denied.

This is not a situation that is simply going to resolve itself. Hackers have exploited remote work setups, but they will not go away when workers return to the office. Instead, they will look for new vulnerabilities to exploit. Don't give them an opening.

- Enable multifactor authentication for sensitive accounts, including email, privileged accounts, remote access, and backups.
- Maintain segregated backups of critical data.
- Install updates and security patches as they become available.
- Evaluate your network for access points and vulnerabilities, such as Remote Desktop Protocol, and take steps to secure your system.
- Educate workers on how to spot phishing scams and verify requests for information, transfers, etc.
- Create a cyber incident response plan and be ready to implement it.
- Stay informed on the latest threats and take precautions to reduce your risk.

Do you need help securing cyber insurance for your clients? Socius provides access to new markets as well as underwriting advocacy. Contact us for assistance.

Brett Klein
Assistant Vice President
email: bklein@sociusinsurance.com
mobile: (203) 830-9442

Cynthia Zimmerman
Executive Vice President
East Coast Cyber Practice Leader
email: czimmerman@sociusinsurance.com
mobile: (954) 804-9450

SOCIUS
SociusInsurance.com

© Socius Insurance 2021. All Rights Reserved.
License# 0D6077