Allied Solutions

Tuesday | August 30, 2022

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

RISK ALERT

Requirements are Changing for Cyber Liability Insurance

SUMMARY

Allied Solutions has learned about new cyber liability insurance renewal requirements. An uptick in data breach liability litigation, large payouts for ransomware attacks, and other cybercrimes have impacted the cyber insurance industry. Because of this, insureds are facing stricter cyber insurance underwriting requirements and increased enforcement of data privacy laws. The persistent increase in attacks has caused cybersecurity to remain a top priority for the NCUA as evidenced by its appearance in their Supervisory Priorities annually since 2014.

INSURANCE REQUIREMENTS

Reduce risks from sophisticated cybersecurity threats and obtain the best policy and quote by taking control of your cybersecurity insurance coverage. Don't wait until cybercrimes have put your institution in financial and/or reputational risk. As your trusted cybersecurity insurance partner, Allied will guide you through the process and help you mitigate your risk exposure by implementing insurance requirements and effective controls including:

- Encrypted air-gapped/cloud-based backups
- Multi-factor authentication (MFA) on:
  - Air-gapped/cloud-based backups
  - Remote network access
  - Remote email access
  - Admin/privileged user accounts
- Endpoint detection and response (EDR) solution in place
- Email filtering
- Encryption on data at rest
- Phishing/social engineering training for employees
- Updating devices to latest version to mitigate log4j vulnerabilities

OTHER RISK MITIGATION CONSIDERATIONS

Incident Response Plan

Have a written and tested incident response plan in place on how and when to notify stakeholders, such as:

- Insurance carrier
- Regulators
- IT provider
- Legal representative
- Public relations leader
- Accountholders

Disaster Recovery Plan
Have a written and tested disaster recovery plan in place including the process for securing backups and a minimal recovery period. Note that recovery should require MFA.

Employee Training
Most security incidents are caused by human behavior, e.g., employee negligence or theft of their login credentials. Therefore, employee training to identify possible security threats is essential.

Phishing attempts and business email compromise (BEC) are common cybersecurity threats that employees should be trained to detect and avoid. Relying on spear phishing and social engineering, attackers are very clever about infiltrating and compromising executives' email accounts. Examples of phishing include manipulating an employee into initiating a wire transfer or communicating sensitive information to the attacker.

Vendor Security
Know what measures your vendors have taken to ensure their own privacy. Review vendor contracts to ensure they are being held responsible with their own cybersecurity insurance policy in the event your financial institution or accountholder information is breached.

RISK MITIGATION RESOURCES

- For more cybersecurity information, visit the NCUA's Cybersecurity Resources webpage.
- For more ransomware information, see CISA's Ransomware Guide.
- Register for Allied's Let's Talk Fraud quarterly webinar series.
- Tap into knowledge from our experts for your loss control efforts by visiting Allied's Risk Alerts Library.
- Connect with an Allied Solutions risk specialist at risk_specialist@alliedsolutions.net.
