Cyber Risks & Liabilities

First Quarter 2021

Top Cybersecurity Takeaways From 2020

According to a recent report from the Information Systems Audit and Control Association (ISACA), cyberattacks currently reign as the fastest growing form of crime. In addition to security and reputational repercussions, these attacks can often cause significant financial disruption—with global cybercrime costs estimated to reach a startling $6 trillion during 2021.

No organizations are immune to cyberattacks. In fact, over half (53%) of respondents from ISACA's report expect to experience a cyberattack within the coming year. With this in mind, it's important to review top cyber trends from the last 12 months and respond accordingly to ensure your organization remains safe and secure in 2021. Here are some of the most common cyber concerns from 2020, as well as best practices for avoiding them:

- **Social engineering**—Cybercriminals implement social engineering scams to manipulate their victims into sharing sensitive information. This manipulation usually occurs in the form of impersonating an individual or organization that the victim trusts, thus making the victim feel falsely comfortable with providing their information. While these scams can happen via text, phone call or email, the latter method (also known as phishing) is the most popular. To keep these scams from wreaking havoc on your organization, instruct staff to always verify the identity of the individual or organization they are communicating with and be wary of sharing any sensitive information over the phone or online.
- **Ransomware**—Ransomware is a type of malicious software that cybercriminals use to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology for the victim. Since ransomware often appears in the form of deceptive links or attachments, encourage employees to never click on suspicious links or download attachments from unknown senders.
- **Software update issues**—Although conducting routine software updates may seem like an arbitrary act, it can make all the difference in protecting your organization. Failing to update your software regularly can create major cybersecurity gaps, making it easier for cybercriminals to infiltrate your systems. That being said, keep staff on a strict update schedule, and consider using a patch management system to further assist with updates.

By keeping these risks top of mind, you can better protect your organization from cybercriminals in 2021.

Provided by SCS Agency Inc

SCS AGENCY INSURANCE

The Importance of Promoting Strong Passwords

Cyberattack methods continue to grow and evolve over time. One specific tactic that cybercriminals frequently utilize is hacking victims' accounts or devices by cracking their passwords.

This tactic is often all too easy for cybercriminals when their targets fail to create strong enough passwords to ward off password-cracking technology or—in some cases—simple guesses.

Nevertheless, cybersecurity experts confirm that establishing an effective password can increase the amount of time it would take for a cybercriminal to hack into an account or device from just a few hours to several years.

Taking this into consideration, password strength should be a top priority across your organization. Encourage your employees to create proper passwords with this guidance:

- **Focus on length**—Choose a password that's eight to 16 characters long.
- **Make it unique**—Use at least two special characters within your password. Don't use family or pet names, special dates or common phrases as your password.
- **Switch it up**—Remember to change your password every 30-45 days.
- **Refrain from recycling**—Never reuse or repeat a password across devices or accounts.

How to Prevent a Malware Attack

Malware is a form of malicious software that cybercriminals deploy via unsafe links, downloaded attachments or other virus-ridden programs with the intention of disrupting normal computing operations, collecting sensitive information and controlling your organization's technology system resources. Malware programs are being produced at an alarming rate and are consistently changing in form and purpose, making detection and prevention increasingly difficult for organizations across industry lines.

According to recent research, nearly 980 million (and counting) malware programs currently exist, while 350,000 new pieces of malware are discovered each day. What's worse, an estimated four companies are targeted by a malware attack every minute.

Consider the following guidance to help prevent malware attacks:

- **Secure your systems**—Take steps to protect your organizational devices from potential malware exposures. This may entail:
    - Using a virtual private network (VPN) for all internet-based activities (e.g., browsing and sending emails)
    - Installing (and regularly updating) antivirus software on all devices
    - Implementing a firewall to block cybercriminals from accessing your organization's VPN
    - Restricting employees' access to websites that aren't secure
    - Limiting which employees receive administrative controls to prevent inexperienced staff from mistakenly downloading a malicious program
- **Educate your employees**—Next, be sure to train your employees on how to prevent and respond to a malware attack. Give your staff these tips:
    - Avoid opening or responding to emails from individuals or organizations you don't know. If an email claims to be from a trusted source, be sure to verify their identity by double-checking the address.
    - Never click on suspicious links or pop-ups—whether they're in an email or on a website. Similarly, avoid downloading attachments or software programs from unknown sources or locations.
    - Only browse safe and secure websites on organizational devices. Refrain from using workplace devices for personal browsing.
    - If you suspect a malware attack, contact your manager or the IT department immediately for further guidance.
- **Ensure adequate coverage**—Lastly, it's crucial to secure proper insurance coverage to stay protected in the event of a cyberattack. After all, even with proper cybersecurity measures in place, attacks can still occur.

  Contact us today to discuss specialized cyber insurance solutions for your organization.