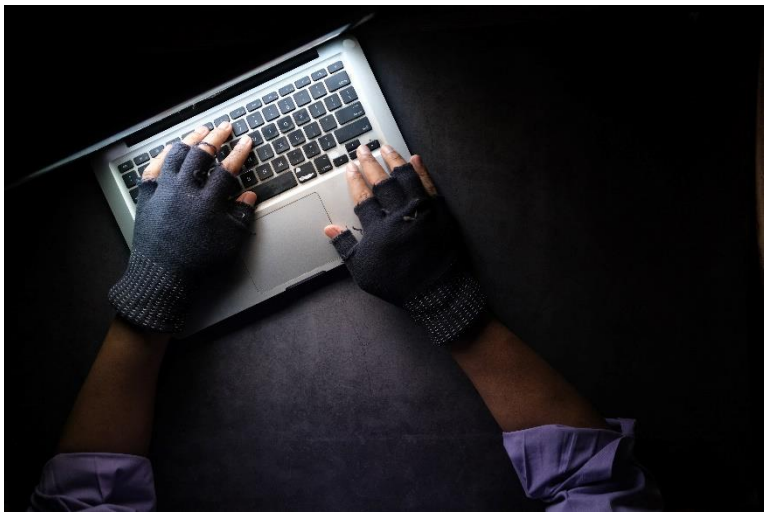
Cyber-attacks: How to recognize, reduce, and respond

As COVID-19 regulations continue to ease across the country, many professionals are eager to visit clients and co-workers face-to-face once again. But the pandemic altered the way individuals choose to behave and communicate, and some may prefer to connect virtually even as in-person services become available.

That means cyber insurance claims, including those related to ransomware, social engineering, and other cyberattacks, remain a risk for engineers and firms. While many engineers may not think they present an appealing target to attackers, insurer data shows the professional services industry experienced the most significant increase in ransomware costs in 2021, with the average claim standing at nearly $400,000.[1]

According to Beazley, the specialist Lloyd's insurer underwriting the stand-alone Cyber Security & Privacy Liability insurance policy available to OSPE members, "employees are typically the first line of defense, but working remotely can make it harder for employees to maintain a culture of compliance. Without a co-worker to converse with, employees are less likely to do a 'sense check' of a suspicious email".

Beazley also reported that the majority of social engineering attacks result in a Business Email Compromise (BEC), where the cybercriminal gains access to an email account. However, cybercriminals were most successful in stealing funds using social engineering techniques to provide fraudulent payment instructions without a system compromise.



[1] Insurance Business Magazine, *"Ransomware attacks ease after peaks in early 2021 – report"*

Recognize the Risk

The table below outlines three types of cyber-attacks professionals should be mindful of:

Social Engineering	Phishing	Fraudulent Instruction
Techniques such as email phishing used to manipulate someone into providing confidential information, such as log-in credentials, or taking other actions that bypass normal security to help the attacker commit theft or fraud.	An email created to look like it comes from a trusted source that is designed to induce a recipient into sharing sensitive information, download malware, or visit an infected website.	A social engineering attack in which compromised email credentials or spoofing are used to induce an employee to make a wire transfer or other electronic payment to a bank account controlled by a cybercriminal.

Reduce the Risk

You don't need to know everything about cyber security to reduce your risk. Beazley notes that modest investment in training and processes can provide outsized returns, reducing the likelihood of falling victim. The following tips are recommended:

- **Alert employees**, particularly those in accounting, finance, HR, and benefits, to be alert to these scams through cyber security awareness training.
- **Establish an out-of-band verification process** to confirm the identity of a person requesting a funds transfer, a change to banking information or payment instructions, or access to sensitive data such as tax and payroll information. We recommend you require voice verification for all changes involving banking information.
- **Don't trust contact details** provided in a request. If the request is fraudulent, the criminal will have supplied fake contact information, too.

  – If the request is by email, call and speak to the person at a number you know to be correct.
  – If the request is by phone, use an email address you know to be correct.
  – Instead of using "Reply," forward the email and type in the email address you know to be correct.
- **Set up Multi-Factor Authentication (MFA)** for remote access to your email system, your VPN, your ACH system, and other sensitive applications. Many platforms now include MFA at little or no cost. This might also be referred to as two-factor authentication (2FA).
- **Tell clients** that you will not change banking instructions without authentication and treat any such request as possibly fraudulent.

Quick tip: Before clicking on links or downloading files, check the full email address of the sender. Cyber criminals are sophisticated, adding legitimate-looking email signatures and signing off with the name of a person who actually works with you, which they may have uncovered through trolling social media and business websites. However, the email address is usually where you can verify the credentials of the sender. Often, it's a small detail that can help you recognize whether it's genuine or not (for example, John.Doe@business.com versus John.D0e@business.com).

Respond to the Risk

BMS recommends that engineering firms who deliver professional services and/or those responsible for maintaining and safeguarding confidential client information purchase additional Cyber Security and Privacy Liability insurance to address their increased risk and exposure.

OSPE members have access to a specialized and comprehensive Cyber Security & Privacy Liability insurance policy that provides first and third-party coverage. It also provides coverage for expert services in the case of an incident, including but not limited to costs involved with a regulatory proceeding relating to the violation of a Privacy Law, including penalties (where insurable), coverage for Business Interruption and Cyber Extortion incidents, and website media liability.

Visit www.ospe.bmsgroup.com for more information & to secure coverage or contact BMS at 1-844-294-2717 or at ospe.insurance@bmsgroup.com to discuss with a broker.

Did you know?

Vyas Sekar, a professor at CyLab, a security and privacy research institute at Carnegie Mellon University told the New York Times, "Like scammers who steal debit card numbers by putting illegal card-reading devices, or skimmers, on A.T.M.s, hackers can easily rip out USB ports and replace them with their own malicious hardware."[2] And while experts are still unsure of how often hacking attacks like these happened, the growing commonality of USB charging ports in places like hotels, public transportation and airports has translated into an increased risk of falling victim to such scams. "People want the convenience of charging their phones and tablets wherever they go," Professor Sekar said, adding, "Obviously I would like it too, but there is a risk."

[2] New York Times, *Stop! Don't Charge Your Phone This Way*

Take the Cyber Security Pop Quiz

As cyber risks continue to evolve, it's important that your knowledge does, too. Below is a short quiz to test your cyber security savviness. **Answers at the end.**

1. **What does the "https://" at the beginning of a URL denote, as opposed to "http://" (without the "s")?**
   a) That the site has special high definition
   b) That information entered into the site is encrypted
   c) That the site is the newest version available
   d) That the site is not accessible to certain computers
   e) None of the above

2. **Which of the following is an example of a "phishing" attack?**
   a) Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
   b) Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information
   c) Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
   d) All of the above
   e) None of the above

3. **Which of the following four passwords is the most secure?**
   a) Boat123
   b) WTh!5Z
   c) into*48
   d) 123456
   e) Password

4. **If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?**
   a) Yes, it is safe
   b) No, it is not safe

5. **If you are in an airport, is it generally safe to charge your phone using a USB wall plug?**
   a) Yes, it is safe
   b) No, it is not safe

Cyber Security Pop Quiz answers: 1. B 2. D. 3. B 4. B 5.