# CYBERRISKS&LIABILITIES

## Email Security Best Practices

Since organizations rely heavily on email to communicate and conduct business operations, cybercriminals commonly target email as an entry point to access networks and breach valuable business data. In fact, 94% of malware is delivered by email, according to Verizon's Data Breach Investigations Report.

Following a cybersecurity breach, organizations may suffer financial, reputational and intellectual property loss. Therefore, it is important for businesses to invest in email security and follow best practices to ensure their data and operations are protected from cybersecurity threats. The following are some email security best practices to prevent and mitigate the risk of email-related cyberattacks:

- **Implement employee training.** Investing in a security awareness training program can help employees navigate email security risks by educating them on potential threats and avoiding situations that could put data and networks at risk.

- **Improve password management.** Many people recycle passwords, making it easier for cybercriminals to compromise data across multiple accounts. Employees should use a unique password that contains a combination of upper- and lowercase letters, symbols and numbers, and change their passwords regularly.

- **Enable multifactor authentication.** Multifactor authentication strengthens email security by adding an extra layer of protection. When users log in to their email account, they must complete an additional step, such as entering a unique code sent by text to their smartphone, to gain access.

- **Be aware of phishing emails.** Cybercriminals often impersonate legitimate senders to steal sensitive information, gain access to operational systems or initiate fraudulent payments. Phishing emails often use language that suggests a sense of urgency and pressure users to complete an action quickly.

- **Encrypt emails, communications and attachments.** Encryption can ensure that emails and their attachments are only read and received by the intended person. It can also help prevent malware attacks through email by ensuring that cybercriminals don't intercept sensitive email data.

- **Avoid public Wi-Fi.** One of the best ways to keep email information safe is to avoid connecting to public Wi-Fi. In addition, investing in a virtual private network, better known as a VPN, can secure an encrypted connection between devices and the internet.

- **Access email only on company-approved devices.** Devices that don't have the proper email security tools and measures may be vulnerable to cybercriminals. Utilizing company-approved devices for all work-related communications can help ensure emails remain secure.

- **Utilize endpoint protection solutions.** Endpoint protection solutions look for critical information included in emails that appears out of the ordinary, such as an abnormal address,

VENBROOK
INSURANCE SERVICES

misspelling of words or suspicious links, and then filters them out before they can be received and opened.

- **Log out of email accounts.** Leaving email open on any device accessible to others can lead to security issues.

- **Back up data regularly.** Although the implementation of sound email security practices reduces the potential for loss, vulnerabilities still exist. Therefore, one of the most important security measures to minimize the potential damage and devastation of a ransomware attack is backing up critical files regularly. Copies should be kept in multiple locations, including on physical hardware and in the cloud.

Implementing a robust email security system and utilizing best practices by employees can help stop email-borne threats, prevent cybersecurity risks and reduce strain on organizations' security teams. For more risk management guidance, contact us today.