Claims Lessons Learned: Cyber Claims

Crimes related to breaches in cyber security have grown exponentially over the past two years. According to an article by ASIS Security Management, losses from cybercrimes amounted to more than $4.2 billion in 2020 due to increasing reliance on technology and mobile devices due to the pandemic. The trends in 2021 appear to be just as alarming: *Forbes* reports that data breaches in 2021 surpassed totals in the previous year and that the hackers have become more targeted in their approach. The tactics they now use are designed to either trick victims into disclosing sensitive information such as bank account PINs and passwords or breach computer systems to directly obtain this information without the owner's knowledge or consent. *Forbes* also indicted that four-fifths of all data breaches in 2020 were financially motivated, meaning the goal of most attacks was to steal money directly or obtain information that could be used to steal from financial accounts easily.

Participants in the Insurance Board program are not immune from this phenomenon. As churches and religious organizations place more reliance on technology, they become increasingly vulnerable to cybercrime.

For example, one participant received a series of email instructions—presumably from one of its ministry partners – requesting a transfer of large sums of money to third-party bank accounts. The emails appeared to come from the ministry partner's finance department and contained the official ministry letterhead as well as all the necessary instructions and signatures. Unfortunately, the transactions were fraudulent as none of the emails and accompanying documents were sent or authorized by the ministry. The originator of the emails was somehow able to access internal documents containing ministry letterhead and signatures from ministry executives. The organization is in the process of recovering the stolen funds, but the financial impact was significant.

In another claim, a church finance manager received an email from someone claiming to be the pastor requesting a change in bank account information for direct deposits. After making small deposits to the account, the church became suspicious when they received an email from the bank telling them that the account was closed. After investigating the transactions, the church discovered that an email scam had victimized them. Fortunately, the church was able to prevent the transactions before incurring a significant financial loss. These claim scenarios are examples of what cyber industry experts call *Phishing*.

Phishing (Oxford Dictionary): *The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.*

According to *Security Magazine*, the financial services and insurance industry has faced a dramatic increase in phishing attacks since the pandemic began in 2020, with almost half of these attempts trying to steal corporate login credentials. There was an average quarterly increase in phishing attacks on mobile devices of 125% during 2020.

It is also an excellent practice to maintain the physical security of your devices, especially when working

Continues on next page

Continues from previous page

remotely. In another claim, a Pastor had his laptop compromised and the perpetrator obtained private information belonging to church members. The church is in the process of finding out how the breach occurred.

According to a report by Travelers Insurance, the transition to a remote work environment due to COVID-19 has contributed to increased cyber-attacks, particularly for small-to-medium-sized businesses. According to Travelers, one of the main reasons is employees who work from home may have less secure routers. Compromised employee devices may put the organization at risk for cybercriminals. Unfortunately, the scenario involving the pastor has been repeated in many businesses since the pandemic began.

According to the *Insurance Journal*, a survey by Travelers Insurance found that in 2020 one in four businesses had been victimized by a cyber event. Many of those businesses didn't have prevention programs like cyber security training, multi-factor authentication, and enhanced cybersecurity monitoring. These prevention measures are essential in protecting churches and religious organizations from cybercriminals, especially as employees in these organizations continue to work remotely.

As trends have indicated over the past two years, cybercrime is a growing threat due to our increased reliance on technology and mobile devices. Businesses including churches and religious organizations need to be continually aware of tactics used by cybercriminals. They will need to make sure they are up to date on protecting their ministries from a cyber event.

Sources: https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/?sh=23c066fb4a36
https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/march/
https://www.securitymagazine.com/articles/96430-mobile-phishing-threats-surged-161-in-2021
https://www.securitymagazine.com/articles/95145-financial-services-experienced-125-surge-in-exposure-to-mobile-phishing-attacks-in-2020
https://www.kaspersky.com/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability

The following are the most common employee mistakes that could leave organizations vulnerable to a cyber attack:

- Opening emails from unknown sources
- Weak login credentials
- Leaving passwords on sticky notes or other visible locations
- Lack of effective employee training to identify cybercriminal tactics
- Not updating antivirus software
- Using unsecured mobile devices

Kaspersky Cyber Security offers the following solutions to reduce and/or prevent cyber attacks:

- Never open emails from people you don't know and avoid opening an unknown attachment or link.
- Employees should use unique passwords and include numbers and symbols for increased security.
- Change passwords regularly, especially if you suspect they may have been compromised.
- Use password managing software for multiple apps, websites and devices.
- Never leave passwords in visible locations.
- Limit accessibility/administrative privileges to company files.
- Require multi-level sign-offs for payments and other financial transactions to combat CEO fraud.
- Provide annual security awareness training.
- Set up automatic system updates and make this a requirement for employees.
- Never conduct confidential transactions using public WiFi.
- Make sure devices are password protected.