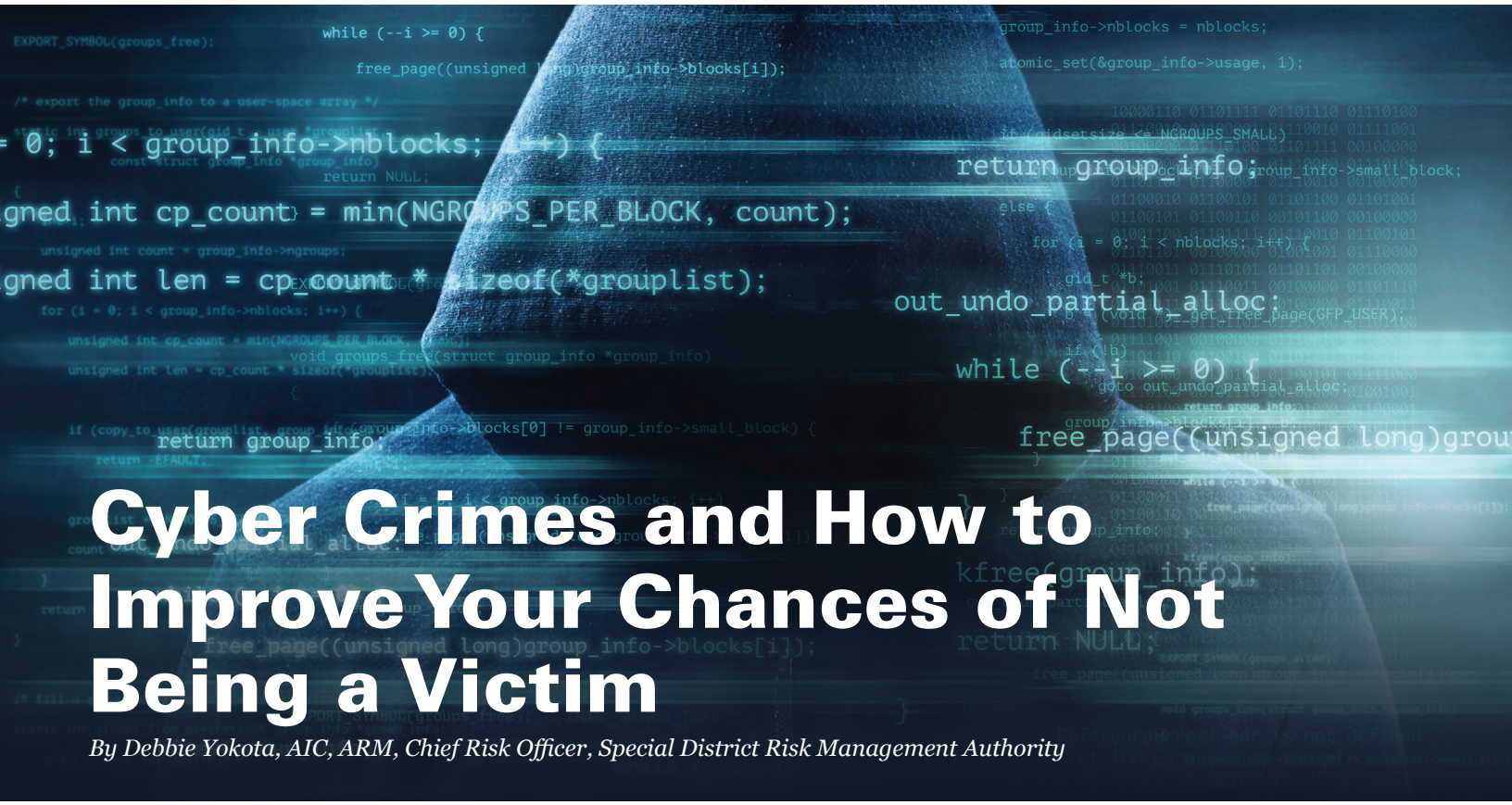


Cyber Crimes and How to Improve Your Chances of Not Being a Victim

By Debbie Yokota, AIC, ARM, Chief Risk Officer, Special District Risk Management Authority

The idea of "computer crime" is not what it used to be. For decades most computer crimes occurred by a hacker cracking into a computer network to complete an unauthorized transfer of funds. Today, one of the most prevalent threats is more direct. Thieves now masquerade as a senior executive, vendor or other trusted associate of a company – tricking an employee into handing over company assets.

This commercial crime exposure is not one that can be addressed simply with state-of-the-art network security, like the computer hacking crimes of the past. Cyber criminals prey on human nature – using trust, an air of authority, and an employee's desire to please the boss or customer to their advantage.

The Threat

The abundance of information available on LinkedIn, Facebook and other social media makes it easier than ever for criminals to collect personal information on executives and employees, so they can use it to convincingly perpetrate this fraud. Often, criminals will begin testing the waters with small amounts of money, moving to larger amounts as no alarm bells ring at a company and the scheme progresses. More often than not, fraudulent instructions direct the victim to send funds to an overseas account or by Automated Clearing House (ACH) – which can make recovering lost assets difficult, if not impossible.

We have seen government agencies who receive an email from an employee at another government agency asking them to send monthly funds by ACH to a new bank account. Later it is discovered that the email did not come from a government employee but was cloned to look like it did. Most banks have no way of recovering ACH funds after 48 hours (domestically) or 72 hours (internationally) once the funds are withdrawn from that bank account.

Addressing the Risk

Combating this online, one-on-one deception can be difficult. The first line of defense for every agency is its employees who should be actively trained to understand and identify these schemes. Agencies should also have prudent verification processes in place, such as requiring out of band authentication of a request before funds are transferred.

Out of band authentication (OOBA) is a term for a process where authentication requires two different signals from two different networks or channels. This type of sophisticated authentication prevents many kinds of fraud and hacking. Out-of-band authentication will effectively block many of the most common kinds of hacking and identity theft in online banking.

Ransomware Attacks on the Increase

Ransomware matters surged in 2019, with the primary tactic being to simultaneously encrypt as many devices as possible within a network. Then, groups started to steal data before encrypting files, which afforded the threat actor two

pressure points (data encryption and data theft/threat of publication) to leverage a ransom payment even if the organization successfully restored their systems through available backups. This new tactic paid off significantly in 2019, prompting other threat groups to begin adopting similar tactics in 2020. Ransom demands, unfortunately, increased exponentially. See Figure 1 below.

Addressing Ransomware Attacks

Most agencies are aware of the risk of ransomware and the need to prepare for an attack. But agencies that have not experienced a ransomware event are uncertain about what actually occurs, which hinders preparation. The first thing an agency should do is keep their software and operating systems updated. Make sure your employees turn on automatic updates when possible. Also be sure to install software to scan your system for viruses and malware, to catch anything that might get through.

Ensure that your employees are using strong, unique passwords and change them often. A password manager program can help you create and remember complex, secure passwords.

Whenever you have the option, enable multifactor authentication, particularly for crucial log-ins like bank and credit card accounts. You should also consider getting a physical digital key that can connect your computer or smartphone as an even more advanced level of protection.

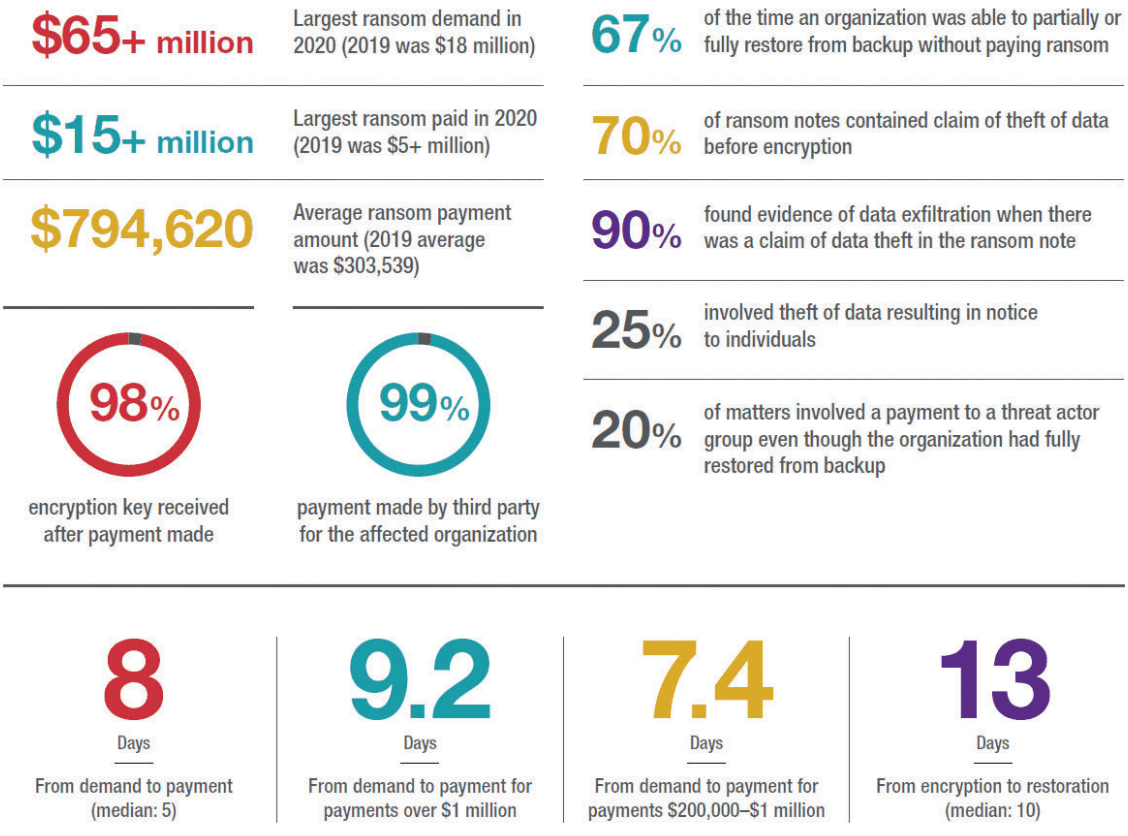
Most of us receive thousands of junk emails after purchasing items online. Have you ever received an email and clicked on the "unsubscribe" button? This is another tactic that criminals use to hack into your computer or other device.

Cybersecurity Challenges of a Work from Home/Hybrid Environment

Agencies across the country scrambled in the spring of 2020 to enable remote work in an effort to keep their employees working during the pandemic. In the haze of that initial move to a remote environment, shortcuts were taken and unfortunate events occurred. For instance, IT teams plugged in unpatched appliances, resources were diverted from threat monitoring, and organizations across the country found unexpected security gaps. Additionally, the pandemic's impact on an organization's finances, personnel, and shifting priorities further redirected attention away from its security roadmap. As a result, unexpected vulnerabilities existed, and security events were not discovered as quickly.

Additionally, where employees are working remotely from their own homes, there are often added distractions. Employees may have to balance work with children or pets who are also in the home, try to perform routine household chores during the workday, or even get distracted by having television

continued on page 40



and other personal electronics at their disposal. Children with access to an open computer connection could inadvertently cause a security incident. Such distractions can add to a risk profile for falling prey to phishing attacks. Employees should be reminded of these issues through training or handy guidelines issued for remote users.

Ways to Improve Working From Home

Companies should have a protocol in place for secured remote access to company networks. Where possible, such connections should be through a virtual private network (VPN), which routes the connections through the company's private network, or another encrypted connection mechanism. Where employees can remotely access sensitive information on the network, VPNs should be configured with multi-factor authentication (MFA) as an added security layer. With MFA enabled, even if an employee's VPN credentials are compromised, an unauthorized actor will be unable to connect through the VPN without a second factor (i.e., a code sent to an individual's smartphone, token, biometric verification, etc.).

Personal devices are more likely to be used when employees are working remotely, and such use presents additional cybersecurity risks given the lack of corporate control over the devices. Where mobile devices (i.e., mobile phone, tablets, laptops, etc.) are permitted to connect to the corporate network, companies should ensure those devices are equipped with mobile device management (MDM) software. MDM software allows the corporate IT Department to manage such devices by ensuring that the devices are configured to consistent standards, scheduling updates and patches for the devices and applications contained thereon, tracking location of devices, and – in circumstances where such devices are lost or stolen – permitting the devices to be remotely wiped.

No Easy Answers

Unfortunately, addressing cybersecurity risk is an always evolving effort – to stay one step ahead of sophisticated threat actors is challenging. However, an organization that invests time and resources to develop plans and take deliberate actions to implement them will find itself ahead of the curve and well positioned to facilitate an efficient incident response. This process starts with an effective risk assessment – understanding who is likely to target the organization; what gaps exist in controls that may detect, prevent, or limit an attack; and which of these threat/gap combinations is most likely to lead to a significant incident if not addressed. From that baseline, an organization should assess and test its incident response plans and take an honest look at its cybersecurity roadmap to understand and implement appropriate measures and controls to help mitigate prioritized risks.

Training of employees is also important. Training should address the increased risk of phishing attacks and other social engineering schemes. In addition to the steps discussed above, employees should be trained not to click on links from any source, even known sources. Cyber criminals are very sophisticated and can send an email that looks like it is from a known vendor, bank or credit card company. Instead of clicking on the link in the email, employees should go to that company's website to make any changes to the account or review any information being sent by that company. Employees should also report any suspicious emails to the IT department.

Regardless of the efforts of the company and the sophisticated security measures put in place to create a safe environment for remote workers, the risk of human error will always exist but keeping these safety protocols in place can help your agency not be a victim of a cyber crime.