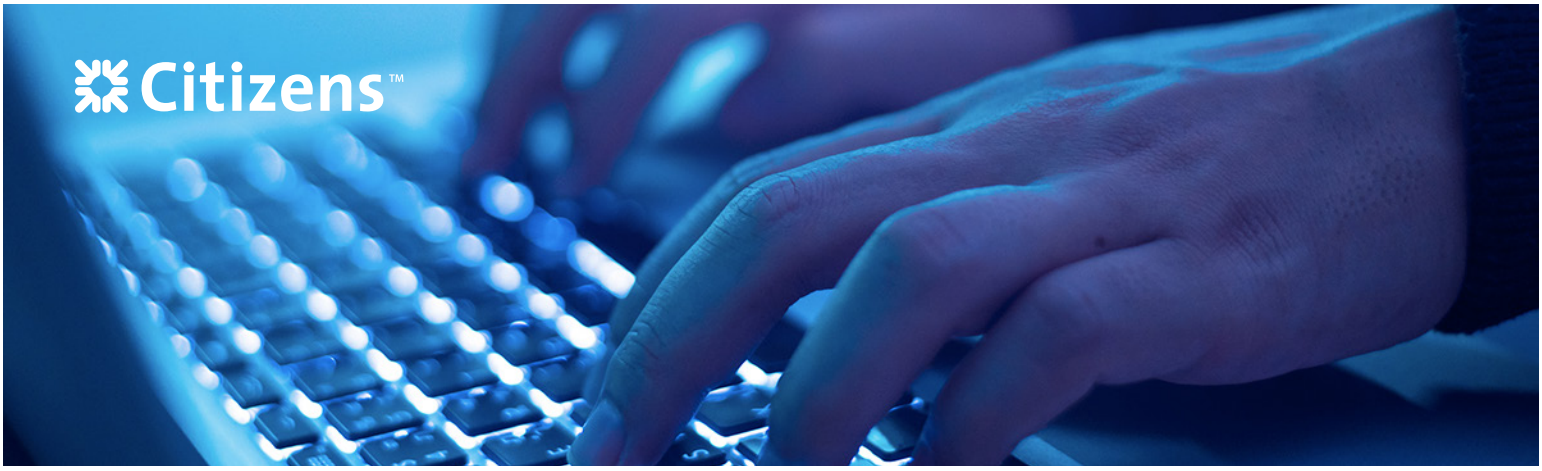


WHAT TREASURERS NEED TO KNOW ABOUT CYBERSECURITY RISK IN AN INCREASINGLY DIGITAL WORLD

By **Matt Richardson** | Head of Treasury Product Solutions, Citizens Commercial Banking

With greater connectivity comes greater potential for cyber risk

Managing cyber risk is not a new priority for treasury, but it's one that demands constant dialogue and attention. While there's been great strides made in developing advanced protection tools for our systems, online banking remains an appealing target for cyber criminals and attacks are on the rise.

Two thirds of companies surveyed experienced some kind of cyber incident in 2019, according to McAfee's The Hidden Costs of Cybercrime report. Without even taking fraud into account, the average cost of downtime for a department is about $590,000. Globally, the monetary loss from cybercrime was estimated at approximately $945 billion in 2020.

The costs of cybercrime

66%
of companies experienced some kind of cyber incident in 2019

18
hours — Average interruption to operations

+$590,000
Average financial impact of downtime to any given department affected by cybercrime

Source: McAfee, The Hidden Costs of Cybercrime, 2020

In treasury management, it seems that as businesses achieve greater digitization and connectivity, in areas like payables and receivables for example, security measures improve but there are also more points of access for cyber criminals to exploit. The COVID-19 crisis was a powerful lesson for many companies in understanding how resilient their systems are, but also how vulnerable they are when faced with securing the future of work and a remote fleet of devices. And as we've learned, security breaches, most often come down to the habits of the individual remote worker.

Familiar strategies, rapidly evolving tactics

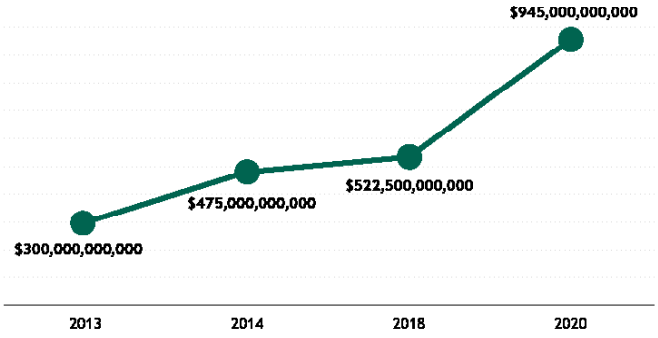
The threats we see having the most impact on businesses today are phishing campaigns, malware and business email compromise (BEC) attacks. These are people-based maneuvers that have been causing damage for years in various forms. Malicious actors are drawn to them because the basic strategy of playing on an unsuspecting victim's gullibility and unpreparedness works.

Phishing was once primarily a phone-based fraud scam. It relies on social engineering and impersonation to extract sensitive information from victims, usually login credentials and personal identities. Today it is largely carried out by email and victims are most often lured to counterfeit websites where they are tricked into surrendering their credentials. Untrained and unprepared for the persuasive tactics, remote workers have been a prime target during the pandemic. The number of phishing attacks doubled in 2020, according to the Anti-Phishing Working Group.

Malware, or malicious software, is right up there in terms of impact and prevalence. It's considerably harder to pull off compared to phishing, but it is much more effective and dangerous. The basis of a malware attack is a virus or piece of software that is been planted on a victim's computer. Once installed, cybercriminals can steal data or take over online banking sessions. There are lots of variations, including ransomware and spyware, and the frequency and sophistication of malware attacks are intensifying.

The other cyber hot spot we are paying close attention to, especially as it affects the financial sector, is BEC. A specialized form of phishing, it has become very common as more companies are moving to remote and virtual transactions. BEC relies on impersonating or stealing the identity of a company employee, usually a senior executive, and tricking victims into exposing valuable information or transferring funds outside the company. Wire transfers and international payments are widely targeted and the volume of attacks is increasing.

Estimated average cost of cybercrime



Source: McAfee, The Hidden Costs of Cybercrime, 2020

New technologies present new opportunities for cyberattacks

The big cyber risk areas right now — phishing, malware and BEC — are rooted in tried and tested social engineering techniques. The speed and sophistication of these attacks, however, are accelerating. And as we look toward the future, the first steps in successful mitigation is going to be understanding how these threats are occurring and the role of technology in fool proofing our systems.

Many companies will focus on new comprehensive tools that improve their systems and operations and have new layers of security built in. Digital payments networks, for example, are greatly enhancing many aspects of payables and they're laden with sophisticated protection measures to mitigate cyber attacks. There will be a lot of opportunity along these lines for businesses to leverage end-to-end solutions that will help them secure their assets and avoid the responsibility and liability associated with cyber risk.

Looking in the opposite direction, the same technologies that have helped businesses move toward digitization and greater connectivity have also created new vulnerabilities. Technologies, such as application programming interfaces (APIs), have made it possible to connect financial services and data in new ways and achieve faster more accurate transactions. But at the same time, there are more openings for criminals to infiltrate and compromise a network.

Similarly, cloud-based email services and applications have revolutionized how many companies do email and created new flexibility and efficiencies. However, these services are showing to be popular targets for BEC scammers who are deploying advanced phishing techniques to exploit service features in order to compromise accounts.

Mobile and personal devices, such as smartphones or tablets, haven't received a lot of attention due to their limited use in commercial banking but this will be an important area to monitor going forward.

Alongside supersized bandwidth, the arrival of fifth generation (5G) wireless technology will introduce a very wide and complicated area of cyber risk to manage. Malware and network manipulation are two of the primary threats highlighted by the FBI.

Businesses must embrace a range of approaches and technologies to protect themselves from cyber risk

The drive to successfully clamp down on cybercrime while supporting business strategy and organizational growth will be equal parts awareness and education.

Companies have been investing heavily in cybersecurity and the tools needed for the job are largely available in many of the online banking, accounting and enterprise resource planning (ERP) systems widely used today. That said, awareness in this space overall will be critical and businesses must be prepared to embrace new technologies and approaches as needed.

In many threat scenarios, the actual integrity of the online banking or security system is usually not compromised, but rather a user has inadvertently become a victim of a social-engineering scam. In this regard, education is of the utmost importance and any worthwhile cybersecurity strategy needs to ensure that cybersecurity is a top-of-mind priority for everyone across the organization.

Citizens™

Key takeaways for mitigating cyber risk

1. **Support organization-wide education and awareness**
   With so much riding on individual liability, it's vital to make sure users are informed about cyber risk, following proper procedures and educated enough to recognize and flag social engineering tactics. It's also very important to keep tabs on the latest trends, tools and technology.

2. **Administer thorough system reviews**
   Invest in understanding your systems, how your transactions affect your operations and where potential cyber risk could be lurking. It's hard to prevent something you don't see or understand. Thorough and regular systems reviews help ensure the right measures, permissions and account management tools are in place and up to speed to address specific threats. This should cover items like system permissions, limits, out-of-band verification (BEC), multi-factor authentication (phishing), dual approval (malware, payments) and separation of duty.

3. **Improve IT best practices**
   Treasury needs to be a proactive partner with IT and work with the technology experts to ensure everything cybersecurity is working as a cohesive whole.

4. **Do your due diligence**
   It's easy to speed toward new technologies and new opportunities, but jumping in before you're ready can leave the door open to unnecessary risk.

5. **Be transparent and communicate clearly**
   Being open with customers and partners about cybersecurity and understanding risk is essential for protecting all sides of the equation — and makes for stronger, more reliable relationships.

Matt Richardson leads Product Solutions for Treasury Solutions at Citizens Bank. He has over 20 years of treasury management experience in sales, product and business administration roles. Learn more at: citizensbank.com/commercial/treasury-management

Find more articles, industry insights and interactive experiences on the latest corporate finance, risk, cash management and M&A trends at: citizensbank.com/insights