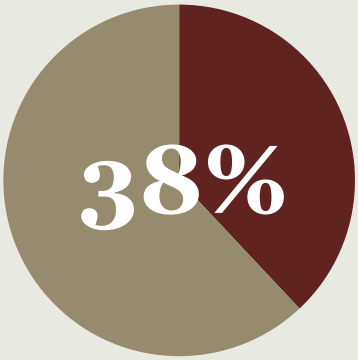
Cybersecurity and payment fraud: The challenge for Treasury

In 2015, **38%** more security incidents were detected than in 2014.



Cybercriminals are stepping up their efforts with more frequent and severe attacks as the world becomes increasingly digital. In 2015, organizations saw a 38% increase in detected security incidents, according to PwC's The Global State of Information Security Survey 2016[1]. As a result, business leaders across the globe are rethinking their cybersecurity programs. Treasury plays a crucial role in these efforts, most notably in building the capabilities required to protect the organization's financial assets and reputation as a good steward of those assets.

? What is cybersecurity?

Cybersecurity is the set of preventative methods used to protect organizational information and resources from being stolen, compromised, and attacked by cybercriminals through the use of computers and the internet. Organizations are becoming increasingly vulnerable to cybersecurity risk due to enhanced technology connectivity and dependency, exposing them to significant financial losses, theft of intellectual property, operational disruption, and reputational damage. Cyberattacks make headlines daily and the numbers are alarming: one breach compromised 80 million customer and employee records while another caused $94 million in financial losses. Unfortunately, it's no longer a question of if, but when, your organization will be targeted.

Cyberattack and data breach methods are constantly evolving; knowing what you may encounter can help your organization begin to protect against it. Companies are targeted in numerous, distinct ways – and Treasury is no exception - from email spoofing to malware and distributed denial of service (DDoS) attacks. An email spoofing attack, or business email compromise (BEC) scheme, occurs when information in an email disguises its true source. For example, a Treasury employee receives an email, ostensibly from a trusted senior executive, requesting an emergency wire transfer to a cybercriminal's account. Malware—software intended to damage system usage or obtain information—could be unwittingly downloaded when a Treasury employee clicks on the wrong link, compromising confidential information such as system credentials. In a DDoS attack, an online service is rendered unusable by a deluge of traffic; if a banking partner were targeted, Treasury could lose the ability to make critical transactions. Cybersecurity is not just an IT issue. It is every employee's responsibility to understand what steps need to be taken to avoid falling victim to a cyberattack

pwc

Why is it important for Treasurers?

Related to the examples above, cybersecurity and payment fraud are key concerns for Treasurers because they are responsible for managing and controlling the organization's financial assets. Many cyberattacks target Treasury's area of responsibility directly, resulting in losses from fraudulent payments, disruption of operations caused by missed payment deadlines, and stolen or corrupted data. In the 2016 AFP Payments Fraud and Control Survey, 73% of finance professionals reported that their company fell victim to payment fraud in 2015, up from 62% in 2014[2]. Additionally, more and more Treasury departments are being actively pulled into IT security and compliance discussions (e.g., PCI compliance). In our experience, companies with decentralized payment environments, distributed bank account structures, excessive numbers of bank accounts and complex bank connectivity models are most exposed to cyberattacks and payment fraud.

To reduce the impact of this threat, Treasurers should ensure the following are in place: sufficient internal controls to safeguard assets, appropriate monitoring around critical assets and systems, complete cash visibility, centralized payment processes, a streamlined bank account structure and bank connectivity model, high levels of automation, and effective employee education around cyber threats and payment fraud scenarios.

Treasury is a key player in preventing and mitigating both the direct impact of an attack (i.e., stolen assets) and indirect impacts including inability to process payments, liquidity constraints and reputational damage. Unfortunately, Treasurers face significant obstacles in implementing effective cybersecurity and payment fraud prevention measures, including the following:

- Attacks are growing in overall sophistication and technological complexity, making it more difficult for the organization's internal monitoring to fully cover the assets Treasury protects.
- Many organizations have limited "real time" cash visibility, decentralized payment environments, excessive numbers of bank accounts, complex bank connectivity models, non-standard processes and far too many staff that have the ability to process payments.
- Bank partner cybersecurity solutions can be inconsistent globally, adding uncertainty and complexity to controls.
- The efficacy of certain security measures is unclear. For example, digital tokens can be just as or more secure than physical tokens but only under certain parameters.

What should Treasurers do about cybersecurity?

Treasury should act immediately to minimize cyber threats and payment fraud risk within their own organizations. Leading organizations employ reliable enterprise-wide frameworks that are continuously reviewed and enhanced to combat new and emerging cyber threats. The overall strategy and identification of critical processes is developed at the enterprise level, with Treasury providing critical input. Treasury should lead efforts in developing a risk-based framework and operational plan that address specific threats related to financial assets and disbursements both within the Treasury function and with other parts of the company that routinely make payments (e.g., AP, payroll, etc.).

The following five key actions can move your Treasury organization toward building an effective cybersecurity risk management approach.

1 Reduce inherent exposure profile

The first step to combatting cyber threats and payment fraud is understanding the company's risk exposure profile. Treasury should identify critical business processes and assets that are at risk by conducting an in-depth assessment of current processes, data, systems and connection points. Once the exposures have been defined, Treasury should take action to reduce inherent risks stemming from process inefficiencies. In our experience, companies can reduce exposure significantly by centralizing payments, reducing bank accounts, limiting the number of people that can make payments, automating processes as much as possible, and streamlining bank connectivity.

2 Establish a well-controlled environment

Given increased risk and several, highly publicized incidents, many Treasury departments are taking steps to tighten controls around cash. Standard treasury controls (e.g., segregation of duties, fraud protection, etc.) can make a substantial difference in combating cyber threats and payment fraud risks; however, controls must be consistently implemented and enforced. Treasury should ensure the appropriate stakeholders (e.g., IT, Finance, Internal Audit) are involved to facilitate the establishment of a well-controlled environment. Companies often fail to completely implement key controls such as token logs for physical tokens, application of two factor authentication, IP restrictions, standard bank services such as Positive Pay, and prior day reconciliations.

When assessing controls, the first consideration is typically protection from an external threat, but internal threats should not be ignored. Current employees are the most cited source of compromise. Therefore, appropriate controls need to be implemented to combat both internal and external fraud, including but not limited to threats that involve current and former employees, current and former business partners, and suppliers.

When implementing the appropriate level of control, Treasurers should aim to build a "suit of armor" while still being able to move and react. This means reviewing current controls around treasury policies, processes, and technologies to determine if appropriate safeguards are in place, but also carefully considering the risk level and the impact on operations. For example, IP restrictions may be too restrictive and present business continuity issues in an environment where staff frequently work remotely. Treasurers must understand the needs of the individual business units and avoid exceptions where possible.

Treasurers face significant obstacles in implementing effective cybersecurity and payment fraud prevention measures

3 Monitor on an ongoing basis

Ongoing monitoring to detect possible breaches is essential. The quicker a breach is identified, the sooner it can be remedied and the potential financial loss curtailed. Treasurers should ensure that prior day reconciliations are performed and determine which anomaly detection solution is best for their treasury technology environment. They should also perform regular bank and user access rationalization. Having many banking partners and bank accounts creates larger exposures. That said, Treasurers need to strike the right balance, taking into consideration such factors as the concentration of counterparty risk and cybersecurity risk presented by limiting banking partners. With respect to user rationalization, the key consideration is whether or not a user needs to have system access.

4 Educate staff

Treasury should develop and conduct training workshops to educate employees on how to prevent, monitor, and mitigate cyber threats. Training should emphasize the diverse source of security incidents, including current and former employees, current and former service providers, and suppliers. There can be limited awareness within Treasury and the business units of phishing and pharming techniques used to infiltrate computers.

5 Prepare for an incident

To prepare for a cyberattack, Treasurers, in coordination with key stakeholders (e.g. IT, Legal, CRO, etc.), should develop incident response procedures and protocols. These procedures should be well documented, communicated to the appropriate employees, and fit within the overall crisis management and business continuity approach.

Companies often struggle to clearly define and communicate when a cyberattack has occurred. During an event, it is essential that facts and decision information move quickly to the appropriate audiences, who can mitigate damage and engage pertinent stakeholders. Realistic mock breach scenarios should be run on a periodic basis, simulating different types of attacks with varying levels of materiality, to test incident response effectiveness and develop the crisis response team's ability to set in motion the appropriate response.

Conclusion

Facing rising cyber threats and payment fraud risks, Treasury can build the capabilities required to protect the organization's financial assets by applying a risk-based framework organized around the four key elements described above: strong controls, ongoing monitoring, staff education, and effective incident response.

The direct benefit of protecting your firm's financial assets is self-evident, but effective cybersecurity risk management by Treasury can also help strengthen relationships with customers and suppliers, build trust with investors, and protect the organization's brand. Not only will your organization be better equipped to defend itself against known threats today, it will also be better positioned to anticipate the risks of tomorrow.

Endnotes:

1. Source: PwC: The Global State of Information Security Survey 2016 <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html>

2. Source: Association for Financial Professionals: 2016 AFP Payments Fraud and Control Survey <http://www.afponline.org/fraud/>

To have a deeper conversation on this topic, please contact:

Hans Candries
Partner, Financial & Treasury Management
hans.candries@pwc.com
+1 (408) 808-2768

Eric Cohen
Principal, Financial & Treasury Management
eric.cohen@pwc.com
+1 (646) 471-8476

Peter Frank
Principal, Financial & Treasury Management
peter.frank@pwc.com
+1 (646) 471-2787

Rob Vettoretti
Managing Director, Financial & Treasury Management
r.vettoretti@pwc.com
+1 (678) 419-4085

Davide di Gennaro
Director, Financial & Treasury Management
davide.digennaro@pwc.com
+1 (646) 471-3151

In addition to our team above, we would like to acknowledge and thank our other contributing authors:

Lindsey Adams
Sr. Associate, Financial & Treasury Management
lindsey.adams@pwc.com
+1 (646) 471-4836

Jeff Frankovic
Sr. Associate, Financial & Treasury Management
jeffrey.frankovic@pwc.com
+1 (646) 471-5494

www.pwc.com/us/treasury