The Corporate View: Tackling the Cybersecurity Threat

Security and fraud prevention have always been vital corporate responsibilities, and central to treasury’s remit. However, the immediacy of these risks, and the potential damage, is growing. As Peter Atuma, Senior Manager, Global Information Security – Governance at Equinix illustrates:

“Defending the organisation against cyberattack is a top priority for us. The nature of cybercrime is constantly changing and every area of the business has a responsibility to protect the organisation and our customers. Ultimately, cybersecurity impacts the business in two primary ways: firstly, the impact on our bottom line, and secondly, the reputational impact. As the global interconnection platform for the world’s leading businesses, the issue of reputational risk is paramount.”

Although cybersecurity is top of mind for corporate treasurers, it is not always easy to know where to start. In this feature, leading corporations Equinix and Prologis, together with Siva Ram, Head of Business Security and Fraud, Global Liquidity and Cash Management, HSBC, share their experiences of best practices in cybersecurity and fraud prevention.

From response to prevention
In many cases, there is a tendency to focus on how best to respond to an attack as opposed to try and prevent it happening in the first place, which often involves deploying existing capabilities. Siva Ram, HSBC, details,

“Treasurers already have a variety of techniques in their armoury (figure 1) to minimise the risk of internal and external fraud, including multi-level approvals, secure integration between internal and bank systems, and daily account reconciliation to avoid or quickly identify unauthorised payments.”

By way of example, Regina Ochev, Assistant Treasurer, Prologis says,

“We have rigorous segregation of duties and a structured accounts payable process with multiple levels of approval on payments before they reach treasury, and then before transmission to the bank. In addition to regular user IDs and passwords, we have implemented multi-factor authentication wherever possible.”

Peter Atuma
Senior Manager,
Global Information Security – Governance, Equinix
Treasurers’ defence against cyber crime

Siva Ram
Head of Business Security and Fraud, Global Liquidity and Cash Management, HSBC

possible, including in our ERP, to control system access. This is an important way of preventing phishing attacks which monitor keystrokes.

“We channel our bank communications via SWIFT, which is closely integrated with our ERP. This ensures consistent processes, controls and integration compared with using multiple banking systems.”

Processes around ancillary data also need to be secured, such as bank accounts (including opening, closing and modifying authorities) and supplier payment details to guard against attacks such as fake supplier instructions. Processes and controls need to be consistent, reviewed and tested regularly and enforced uniformly across the organisation.

As Duang Wollring, European Treasurer, Equinix describes,

Fig 1. Treasurers’ defence against cyber crime

Source: 2017 AFP Payments Fraud and Control Survey

- Cybersecurity is the no. 1 concern for 82% of treasurers
- 78% of corporations have been hit by payment fraud in the past year
- 65% of this originated from outside the company

1. Perform daily reconciliations
2. Adopt a stronger form of authentication or added layers of security for access to bank services
3. Ensure disaster recovery plans to include the ability to continue with strong controls
4. Upgrade the authentication procedure/devices used to access our company network
5. Restrict company network access for payments to only company-issued laptop
6. Restrict company network access for payments via mobile devices (laptop, tablets, phones to emergency situations)
7. Dedicate a PC for payment origination (with no links to e-mail/web browsing/social networks)
8. Replace proprietary bank connections with secure access through the SWIFT network
9. Other
“From a treasury perspective, we take an end-to-end approach, identifying every process and task that could create a vulnerability, and explore how we can bolster our defences. For example, we work with our internal and external partners to ensure that every step in the payments process is encrypted. While we have not experienced a breach due to inadequate encryption, it is essential to be a step ahead of the fraudsters, rather than waiting for something to happen.”

In many cases, fraudsters target subsidiaries or branches where controls may be less rigorous. Centralisation can be a valuable way of overcoming this risk, as Duang Wollring emphasises,

“Centralised structures can help by enabling a standardised approach to processes and controls, and create common goals. Centralised business functions such as treasury and shared service centres also provide sufficient scale to implement segregation of duties.”

Siva Ram, HSBC continues,

“Crucially, it is far easier to apply consistent processes and controls and ensure that staff training

is up to date in regional or global treasury centres or SSCs than in multiple locations. Where this is not feasible, ‘virtual’ centralisation through a common technology hub ensures that processes and controls are enforced consistently.”

Training and culture
While the right technology and processes have an important role to play in treasury’s defence against the threat of cyberattack or fraud, training and
empowering employees is equally important in defending the company against internal and external cyberthreats. Regina Ochev, Prologis explains,

“All employees are encouraged to take a personal role in protecting the company’s assets, and people are empowered to question actions that they consider unusual including holding payments while conducting call-back confirmation procedures and escalating unusual transactions to management.”

As Siva Ram, HSBC suggests,

“In addition to rigorous, uniformly applied processes and controls, education and training is essential so that users are equipped to recognise potential attacks. For example, most unauthorised access is committed using impersonation fraud (such as email fraud, CEO fraud etc.) or phishing where it is user behaviour rather than controls on infrastructure, that creates the vulnerability.”

Peter Atuma, Equinix continues,

“Phishing is probably the most common form of attack, and the incidence and severity of these attacks is increasing. As with other cyberthreats, awareness and education is key. We have mandatory training for all staff to help them identify phishing attacks and understand what to do, including some specific education for finance professionals. We also test all staff with dummy scam emails to determine how vulnerable our workforce is to common attacks, as well as enabling us to refine our education and training.”

Regina Ochev, Prologis concurs,

“We provide extensive, company-wide training on the changing nature and severity of external threats, as well as how to guard against internal risk of fraud. This is essential to prevent people from becoming unwitting targets of phishing attacks etc. and we test our controls regularly.”

Training cannot be a one-off activity, but a regularly updated, regularly delivered programme tailored to different types of user. Duang Wollring outlines how Equinix have approached this,

“Ensuring that staff are aware of cyberrisks, but also understand and comply with business processes and controls is particularly important in treasury and our shared service centres given the nature of their responsibilities. With this in mind, Equinix makes education mandatory at all levels of the company.

“Creating the right culture of diligence is vital so that every employee recognises their role in protecting Equinix and our customers. This includes a culture of constant improvement, so that employees identify where processes or controls could be enhanced.”

**Rapid response**

However effective the processes and controls that are in place, and however well-trained the workforce, every company could be attacked. Consequently, ensuring a fast and appropriate response to suspected or actual attacks is essential. Many companies still have a cultural issue that staff are unwilling to raise the alarm for fear of blame. Siva Ram, HSBC advises,

“In the event of an actual or suspected cyber breach or fraud event, acting quickly is of the essence. All staff involved with managing transactions or data in treasury therefore need to be able to recognise these events and know how to respond. Simulating attacks, not only in central or regional treasury centres or SSCs but in other parts of the business where cash and treasury management activities take place can be a very valuable way of overcoming users’ reluctance to act, practising responses and identifying areas for further exploration and resolution.”

Every organisation must be prepared to manage the impact of a breach or fraud event in a way that is prompt, proportionate and appropriate to the

---

**Duang Wollring**

European Treasurer, Equinix
company’s risk appetite. Siva Ram HSBC highlights some of the questions that need to be addressed,

- “In the case of ransomware, under what circumstances would you pay hackers? How much? When? How? For example, you would not be able to pay using normal payment channels, so are you set up for, and prepared to use cryptocurrencies?

- In the case of a data breach, do you know where your data is located? How would you restore services in the case of an attack?

- What would you need to do to set up a skeletal treasury function? A serious attack could mean entirely new hardware and operating software may be required if this was compromised: are you prepared for this?”

**Collaboration and information sharing**

Treasury is not alone in tackling the cybersecurity threat. As Peter Atuma, Equinix advises,

“It is essential that IT works closely with business functions such as treasury to create a cohesive approach to cyber defence and work collectively as good corporate citizens. We work beyond organisational silos and prioritise our security activities according to urgency and the potential scale of impact.”

The need for collaboration extends not just within the organisation but beyond. Duang Wollring, Equinix urges,

“We must all work together to defend and protect our organisations and the digital supply chain we operate across against the threat of cyberattack. This includes banks, technology providers, industry peers, customers and suppliers. Information sharing and industry collaboration is a particularly important way of strengthening our collective defences.”

Taking a leadership role in cybersecurity is an important way in which treasury can elevate its reputation and influence in the organisation, as Regina Ochev, Prologis concludes,

“Our treasury function evolved from a traditional cash management function to a far more influential team that plays a major role in cross-departmental projects such as cybersecurity, financial reporting, and exploring innovations, such as robotics, blockchain and smart contracts. Increasingly, we are part of the wider business ecosystem, partnering the business to help innovate whilst protecting the business.”

**Notes**

1. The Business of Treasury, Association of Corporate Treasurers, 2017
2. AFP Payments Fraud and Control Survey, 2018
3. Payments Fraud and Control Survey, Association of Finance Professionals, 2018