Fighting Cybercrime and Fraud:

A Treasury Imperative

By **Eleanor Hill**, Editor

As instant payments grow, digital commerce spreads, and artificial intelligence rises, staying a step ahead of the cybercriminals is increasingly tough. But with access to highly sensitive data, and as guardians of the company's cash, treasurers can no longer hide behind the IT department when it comes to cybersecurity and fraud, writes Eleanor Hill, Editor.

Levels of corporate fraud are at an all-time high, largely because of the growing sophistication of cybercriminals. As such, fraud and cybercrime are no longer one-off instances of bad behaviour. They are front and centre risks for every business, 24/7/365.

In fact, according to the 2017/18 *Kroll Annual Global Fraud & Risk Report*, 84% of companies surveyed worldwide experienced a fraud incident in 2017, 86% reported at least one cyber incident, and 70% reported security incidents. The impacts of such attacks are well documented – from financial losses and reputational damage through to loss of competitive edge and low staff morale.

If all this wasn't worrying enough, corporate treasury departments are now prime targets for cybercriminals and fraudsters. "Treasury's trove of personal and corporate data, its authority to make payments and move large amounts of cash quickly, and its often-complicated structure make it an appealing choice for discerning fraudsters," says a 2017 report by the Economist Intelligence Unit, sponsored by Deutsche Bank, called *Third-Party Risks: The cyber dimension*.

"These sophisticated cyber-criminals use social engineering and inside information gleaned from lengthy reconnaissance within a given company's systems to execute high-value thefts. They understand that the ability to access payment infrastructures and bank communication channels is extraordinarily powerful. They know that treasurers rarely control the IT security infrastructure they use. And given the nature of some successful attacks, hackers also seem to understand that most treasuries contain junior staff who can be pressured into infringing rules," the report notes.

This is precisely why treasury professionals can no longer afford to pass the buck when it comes to cyber and fraud defences (it is worth nothing here that the two go hand-in-hand even if fraud is not always committed through cyber channels). As Jean-Marc Servat, Chair of the European Association of Corporate Treasurers (EACT), notes: "Treasurers are not only accountable for the largest payments in the group, they are also perceived as trusted risk-managers, so they absolutely have to be on top of cybercrime and fraud."

Servat concedes, however, that attack vectors and targets are constantly changing, which makes it tougher for the treasurer to stay one step ahead of the criminals. While it is undoubtedly true that the criminals are getting more creative, Nadya S Hijazi, Global Head of GLCM Digital, HSBC, says that there are three main types of cyberattack that corporate treasurers should be on the lookout for.

Threats to treasury

The first such threat is business email compromise, which is typically where the cybercriminal sends emails purporting to be from someone within the company – often the CEO or CFO – by compromising or spoofing company email accounts. These attacks are extremely common and highly successful, she says.

"There is a tendency to think that business email attacks are still very crude and therefore easy to spot. But that couldn't be further from the truth. Cybercriminals, especially those targeting corporates, are extremely sophisticated. They will have undertaken thorough reconnaissance on the company, current deals being undertaken, and the people in key positions within the organisation. As such, they will also know who has the authority to sign off on payments," explains Hijazi.

The second attack vector that is a particular concern for treasurers is phishing, in particular voice phishing or 'vishing'. This involves using social engineering techniques over the telephone, leveraging information in the public domain to either impersonate an organisation, such as a bank, or an important person within the company. The aim, says Hijazi, is typically to get employees to reveal sensitive information, unknowingly make urgent payments to fraudulent accounts, or change data within the company's system – such as bank account details for a supplier.

"Again, these attacks are very sophisticated," she cautions. "The cybercriminals can often replicate the phone numbers of the banks when calling, so that it looks like a genuine call. Because they are so convincing, and hit all of the right trigger points, the success rate of vishing attacks can be as high as 85-95%."

Ransomware is the third threat that treasurers would do well to keep a close eye

Nadya S Hijazi

Top tip: Keep ransomware at bay

"Ransomware often targets weaknesses in operating systems, such as Windows, which is why it is vital to install software updates as soon as they are released," notes Hijazi.

Giacomo Baldi

on. "The corporate sector saw a growing number of such attacks in 2017 and some very high-profile organisations fell victim to extortions in this way. And although few companies will admit to it, the ransoms are often paid," says Hijazi.

Getting involved

Being aware of common attack vectors is extremely useful, but treasurers also need to know how to try to prevent cybercrime, and what to do as and when an attack is successful (which is more or less inevitable). This kind of proactivity is often lacking in many treasury departments as a result of gaps in knowledge, unclear responsibilities, and resource-constraints.

As David Watson, Head of Cash Management Americas and Global Head of Digital Cash Products, Global Transaction Banking, Deutsche Bank, explains, "While most treasurers show an interest in cybersecurity as a topic, many don't necessarily understand what role they ought to play on the front line of defence."

This is echoed by Giacomo Baldi, Treasurer, GE Grid Solutions & Power Conversion, who says: "At General Electric, we have a company-wide focus on cybercrime. The treasury department is in touch with IT to ensure that all of the systems are robust, but we don't have a specific cybercrime protocol within treasury, as such."

As the treasurer becomes more and more visible in the business, however, he or she will need to be a driver of cybersecurity controls – rather than leaving it all to the Chief Security Officer (CSO), says Watson. To do that, treasurers need to look beyond their job description and start to really embrace their role as a strategic business partner. "They also need to have the confidence to stand up in front of the CFO and board and explain that, since they are responsible for the safety of the firm's capital and assets, they need to be given the appropriate tools to accomplish that," believes Watson.

An action plan

That said, what exactly should treasurers be aspiring to when it comes to best practice around cybersecurity and anti-fraud systems, processes, and mind-sets? Furthermore, what does the popular 'prevent, detect, respond, recover' mantra look like in a treasury environment?

Bob Stark, Vice President of Strategy at Kyriba, recommends the following four-point plan as a sound basis:

1. **Data security** – including an assessment of treasury system vendors' risk governance programmes. "Treasurers need to think carefully about the technology providers they place their trust in, including treasury management systems hosted in the cloud. Trusting that your vendors are practising effective self-governance is an unacceptable risk," he observes. Deutsche Bank's Watson adds that: "As soon as you establish linkages with suppliers, business partners, and to some extent, technology vendors, the security of their systems, as well as their risk management protocols, also becomes of relevance to you. When you have a large-scale supply chain, every step in that chain has both technological as well as human capital risks."
2. **Application security and user control** – this involves ensuring log-in protocols to treasury systems align with internal information security practices such as single sign-on, multi-factor authentication, and IP filtering, says Stark. Watson agrees, adding that, "keeping a firm handle on user control is

> *Treasurers need to think carefully about the technology providers they place their trust in, including treasury management systems hosted in the cloud.*

Top tip:
Cover all fraud bases

"Fraud can be internal as well as external. Depending on the surveys one reads, fraud from internal parties range from 10% to as high as 40% of total attempts. It is critical to focus efforts on combating cybercrime, but not to the point that internal fraud protections are under-emphasised," says Stark.

Top tip:
Prepare for the worst

"Assume that internal and external fraudsters know information about you and your organisation. A fraud attempt is typically made after such research and profiling have occurred," says Stark.

a basic, but very effective, measure in tackling cybercrime and fraud. Regular user reviews are imperative and as soon as someone leaves the company, their access to corporate systems should be deactivated immediately."

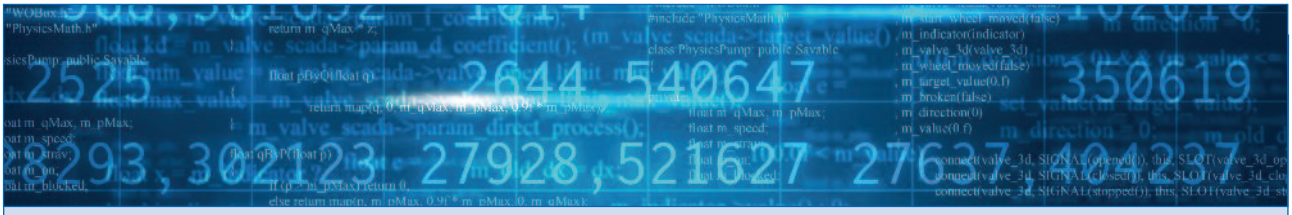
3. **Standardised payment controls** – so that initiation and approval of payments is consistent across all payment types, in all geographies, and by all users. Exceptions to such a policy, including different processes for treasury vs. ERP systems or a different set of rules if executives request payments, sharply increase the risk of fraud. "Centralisation of payments is a great example of a process that will help standardise payment controls and authorities to ensure that all payments are initiated, reviewed, approved, and transmitted in a consistent way. This helps minimise risk in addition to the technology that enables the payment factory and resulting intercompany transactions that support it," says Stark.
4. **Payment screening** – this, Stark advises, should be carried out against both external watch-lists (such as OFAC in the United States), as well as internal scenarios that align with the organisation's global payment policy.

In light of the above, having an efficiently run treasury function, where reconciliations are performed in a timely manner can also be a significant help in protecting and detecting fraud, says Hijazi. "Ensuring different people within the treasury or wider finance function are conducting daily spot checks on transactions can also be a good way of staying a step ahead – since a different pair of eyes may notice something suspicious."

People are the key

In addition to best practice around systems and workflows, ensuring treasury staff are up to speed is another vital tool in the prevention and detection of fraud and cybercrime. As Servat explains, "the digital world has opened up new avenues for financial crime; but underneath, it's still all about people. Take CEO or CFO fraud, for instance. That revolves around impersonation and trust, albeit misplaced."

Since people are the weakest link in any company's cybersecurity and fraud framework, "the power of cybercrime prevention training, retraining and testing should not be underestimated," says Watson. This means not just company-wide training, but specific training for



Tackling supplier fraud

One of the most common types of fraud that treasurers will see is supplier fraud. "At GE, we've had at least three or four attempted frauds – where the fraudsters tried to divert funds by changing the bank account details of one of our suppliers," confirms Baldi.

"As a result of these attempts, we have improved the controls in our sourcing department around changing supplier details, especially bank account numbers. Now, no changes can be made to such details without additional checks, such as directly calling the usual contact at the company on the telephone number that was already in our records, or via the switchboard number that appears on the supplier's website."

Similarly, Servat advises that, "any attempt to modify master data held about suppliers must undergo rigorous checks. Something seemingly innocuous, such as changing a telephone number, could be the start of a long game plan for a fraud, winding up with changing the IBAN associated with an account. Fraudsters are incredibly patient and will keep trying different routes to get what they want. Layered controls around the company's master data are therefore vital."

Stark adds that: "one of the most common fraud blind-spots is assuming that payment controls such as separation of duties and limits will prevent payment fraud. Controls should support payment scenarios, such as whether the supplier's bank account instructions were recently updated or if the BIC that the payment is being sent to matches the country in which a supplier is located."

treasury personnel. Contract workers should not be forgotten, either.

In addition, "test emails containing links that employees shouldn't click on are a classic but reliable way of checking how on-the-ball your department is. Some companies have started taking this to the next level and if an employee clicks on the link in the test email, they are immediately taken to a training portal. It's not just about email, though, training is needed for all communication tools, including the telephone," adds Watson.

As much as training and controls are vital in the fight against cybercrime and fraud, Servat thinks there is an element of gut instinct that is very important too. "In the days before digitisation, we used to have to conduct business based on mutual trust and our own impressions about someone. Through decades of experience, we had derived ways of working and practices to reduce the risk of fraud. Those practices are now partly obsolete, as everything is done via a computer. We no longer use those classic instincts – and perhaps it's time to get our fraud reflexes updated," he suggests.

Another important people-related aspect of cybercrime and fraud prevention is having the right culture within the treasury and wider finance function. As Hijazi explains, "Cybercriminals often target mid-level managers because they are typically the ones who don't necessarily feel confident enough to step up and challenge requests coming from the CFO or CEO, or someone pretending to be them. Cybercriminals play on those insecurities and assume that people will be too embarrassed to ask questions of their superiors."

Baldi agrees that corporate culture plays a huge role in helping to mitigate fraud and cybercrime. He says that it's not just about setting the right tone from the top, though. "For me, it's critical that there is greater integration between functions – especially between shared service centres or centres of excellence and the rest of the business. Often these units operate in isolation, which makes it harder to spot potential frauds."

On a related note, establishing a good working relationship with the Chief Information Security Officer (CISO) and/or CSO is also important. As Watson points out: "If the treasurer can help the CSO to have a better understanding of where the money flows, why it flows, when it flows, and how it flows, then the CSO will be better equipped to help protect company funds from cyber-attacks." Stark agrees, saying that: "treasury should not be an island; it is vital to collaborate with information security."

Likewise, Servat believes that working closely with the IT team is now more important than ever. "The treasurer should co-operate with IT department to help set up awareness programmes for their teams, with practical examples to work through." Moreover, "working with IT to find a white hat or consultant to conduct penetration testing can also be very effective," in the prevention of cybercrime, he believes.

It is worth noting here that the most effective penetration testing involves the use of simulations to determine what type of damage could result if IT systems are attacked from both internal and external sources. Somewhat worryingly, the latter is often neglected, with 33% of companies only performing internal penetration testing, rather than a combination of both, according to the Deutsche Bank/EIU report.

Respond and recover

While prevention and detection measures are imperative, when the worst happens, it is important for treasury to have a dedicated

Bob Stark

Top tip: Getting funds back

"The sooner an organisation informs the bank that funds have gone missing as the result of a cyberattack or fraud, the better the chances are of getting that money back. After 24 hours, the probability of seeing those funds again is significantly reduced. Therefore, the more centralised and connected the treasury function is, the better," says Hijazi.

> *Another important people-related aspect of cybercrime and fraud prevention is having the right culture within the treasury and wider finance function.*

David Watson

Top tip: Leverage legislation

Legislation is catching up around cybersecurity. "GDPR, for example, is a positive force in the industry because all organisations holding data will need to conduct an impact assessment. The process of doing so should help them to spot any weak areas in their protection of the data they hold," says Servat.

departmental action plan in place, including a clear chain of escalation. One that can be accessed even when systems are down – such as in the event of a ransomware attack.

After all, one of the most devastating aspects of ransomware is simply how pervasive its impact can be, explains Hijazi. "Systems will be shut down and taken offline in order to stop it spreading, leaving treasurers with no online access to bank accounts and therefore unable to make payments over the internet. It's no use thinking that using your company laptop from home will be fine – that won't work either."

A business continuity plan (BCP) that specifically covers how payments will be made in the event of a ransomware attack is therefore vital. "Some banks will be able to assist with making certain payments on behalf of corporates as a workaround, but this is not a bullet-proof solution," she observes. Having a list – on paper or on your mobile phone – of contacts at the bank is also advisable in such a situation.

In addition to this departmental action plan, being plugged in to the IT team and CSO will once again be critical to ensure treasury is able to properly respond to and recover from cyberattacks. "Most organisations will have a Security Incident Event Management (SIEM) programme in place, which is a combination of internal processes as well as investment in tools and services from third parties such as Splunk and FireEye," says Stark. "Treasury needs to be part of this programme to ensure their requirements are included in the planning and coverage."

Stark also advises that treasury's cybersecurity and fraud prevention framework should be evaluated frequently in concert with the organisation's information security team. This, he says, will ensure treasury has the latest information on cyber threats, such as cybercriminals' use of artificial intelligence to exploit organisations' weak points.

A collective effort

Elsewhere, sharing information between corporates about successful and attempted cyberattacks is another important tool in the fight against cybercrime, according to Servat. "The EACT has set up a working group to do just that, with the aim of creating a place to share knowledge and information around cybercrime – or perhaps even a hotline for reporting cybercrimes and frauds, after calling the relevant authorities," he comments.

Understandably, some corporates are hesitant to admit to breaches or frauds but a joined-up approach to sharing information in a timely manner is vital. "You can be sure that the hackers are sharing information among their community very rapidly, so we must do the same," says Servat.

Thankfully, sharing of information is gradually becoming easier as cybercrime is now becoming a less taboo subject. Transparency around the topic is being praised by the press, the public, and even shareholders. As Servat notes: "It is far better to be open and upfront about any issues than for the market to find out later.

"Moller Maersk took this approach last summer when they were hit by a NotPetya attack. They made sure to communicate to the market an estimate of the financial impact ($300m in lost revenues) and have also talked openly about how they resolved the issue and how they have improved their system recovery processes since."

A helping hand

As much as corporates may be thinking about working more closely together to help beat the cybercrime and fraud, surely the banks have a role to play here too? Baldi is not the only treasurer out there thinking that "the burden of tackling financial crime falls very much on corporate shoulders, rather than on the banks." He adds that, "it would be nice to see a little more support from that corner."

Naturally, some banks are stepping up to the mark. "At HSBC, we are very passionate about helping customers to understand what forms cyber threats may take, and what best practice cybersecurity looks like. We are more than happy to have very candid discussions with treasurers and provide suggestions on best practices. Of course, we also invest heavily in our own systems to ensure they are as robust as possible," says Hijazi.

And Watson feels similarly about

Deutsche Bank's efforts, saying that "In many ways, cybercrime is an evolution of the old-fashioned bank heist. A century ago, banks had to have a secure vault that was impossible to crack, as well as the thickest bars on their windows, in order to protect customers' assets. Today, the premise is the same – but the 'vaults' are typically digital. And while the criminals might not be physically present in the branch, they still wear 'disguises' – pretending to be people who they're not or using fake signatures, for example."

Watson adds that, "banks absolutely need to stay ahead of the curve when it comes to cybersecurity and we have a significant role to play in helping our clients to do the same. That's precisely why we recently sponsored the aforementioned EIU report that looked into the state of treasury cybersecurity and aimed to identify what could be done to improve it."

While these individual bank efforts do not go unnoticed, treasurers would still like to see more co-ordinated action among the banks. "It would be great to see more cross-border co-operation between banks in the fight against fraud. If there were international blacklists of fraudulent payees or IBANs, for example, that would be incredibly helpful," explains Servat. He admits, though, that "with all the privacy issues around data, this may be more of a pipe dream for now."

Top tip:
Check and check again

"When it comes to fraud prevention, my best advice is not to take anything for granted. Double or triple check anything that looks even remotely suspicious. And never change bank details for a supplier without doing the proper checks first," says Baldi.

Emerging trends and future-proofing

The point around data privacy is an interesting one (particularly in light of the EU's General Data Protection Regulation) – and, in a way, highlights an evolution that is taking place in the nature of cybercrime. Namely that data is becoming an ever-more significant prize for hackers, who are increasingly part of organised crime rings.

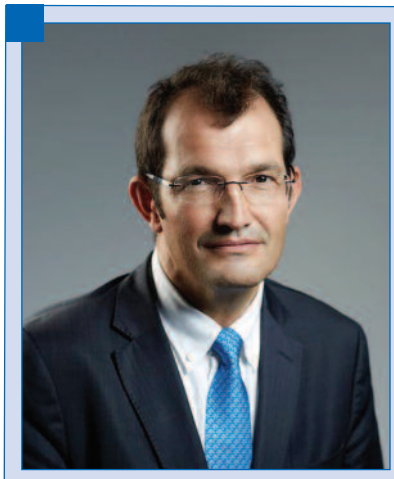
"Treasurers therefore need to be alert to the fact that data is a new form of currency – one that needs to be protected as much as traditional currencies," Servat notes. Getting used to this notion will be vital for treasurers who wish to better understand their growing role in the prevention of cybercrime.

Other emerging trends to watch include the use of open application programming interfaces (APIs), which is only going to increase in the years ahead. According to Watson, this will require treasurers to have different security protocols – and skills – in place. Treasurers, he says, will need to be well aware of whom they are opening an API door to and why.

"PSD2 will also give rise to new potential cybercrime considerations, since third-party access will be the order of the day and the use of bank account aggregation services may well increase. In such an intermediated environment, treasurers will need to know who is accountable for any data breaches that may happen and how to escalate any incidents with the third-party provider," he cautions.

Instant payments will also increase the risk in the cybersecurity and fraud landscape, given the timeframes involved. As Stark warns: "Your bank cannot save you if unauthorised payments are sent. This becomes especially important with faster and real-time payment initiatives."

Thankfully, the cybercriminals are not the only innovators, and new prevention and detection tools are emerging to help tackle the evolving threats associated with instant payments. "Many technology providers are building complex algorithms and robotic processes to deliver real-time payment detection, so that suspicious payments can be halted and investigated before they are



Jean-Marc Servat

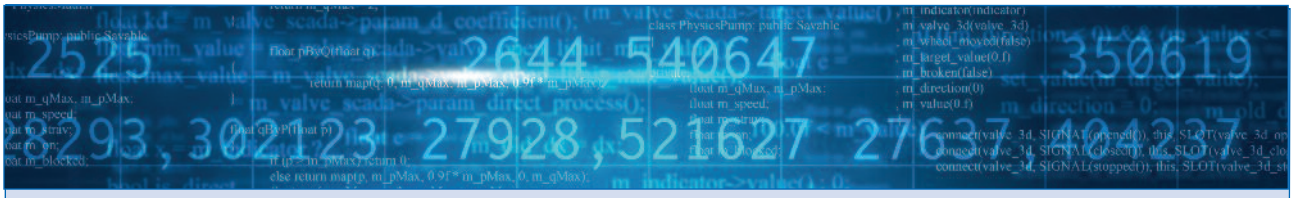
> *It would be great to see more cross-border co-operation between banks in the fight against fraud.*

transmitted outside the organisation," says Stark. "Over time, machine learning will be built into these screening rules so that the software learns from the data it ingests."

Supplier bank account verification is another trending area, according to Stark, as CFOs and treasurers want suppliers to authenticate the payment instructions before payments are remitted. Again, this is becoming especially important as real-time payment technologies increase in popularity.

Staying ahead

But, of course, technology is only part of the equation. "To effectively tackle cybercrime and fraud, treasurers need to look at three components: technology; processes; and people. Those components cannot be looked at in isolation, however. Understanding the interplay between them, and plugging any gaps, will be critical to staying on top of cybercrime and fraud going forward," Servat concludes. ■



How to combat cyberattacks and fraud

DO

1. Put in place a strong contingency plan that covers how payments will be made in the event of systems being shut down due to a ransomware attack.
2. Work closely with the IT and security teams to understand possible weaknesses in treasury processes and systems and how to address them.
3. Undertake daily reconciliation of accounts and know who to call in the bank if funds need to be recalled
4. Invest in training for treasury staff around cybersecurity especially phishing, vishing and other forms of social engineering.
5. Work in partnership with your bank(s) to formulate a contingency plan that outlines what actions will be expected of the bank if/when a cyberattack happens.
6. Learn about cryptocurrencies and how to procure them, in case the company is subjected to a ransomware attack and agrees to settle.
7. Have a process for validating large value payments. HSBC, for example, allows multiple authorisers and signature groups on its online banking platform for commercial customers.

DON'T

1. Never act on information in an email or letter without double-checking it. Phone a known contact at the organisation, or the relevant person within your own organisation if it is an internal communication, and ensure the details are correct.
2. Never change a supplier's bank account details without triple-checking any changes first – again, call a known contact at the company.
3. Never give out any codes or passwords to anyone over the phone – especially someone saying they are from your bank. A real bank will never ask for this kind of sensitive information.
4. Never think that caller ID is a reliable indication of who you are speaking with. Phone numbers can be easily spoofed, so take nothing for granted.

Source: Nadya Hijazi, HSBC