In the area of cash management, security and controls are fundamentally important. From payment fraud to the risk of error, corporate treasurers need to be aware of the different threats that can result in financial loss. "It's inevitable when you are moving money around that people will be thinking of ways they can defraud you," observes Chris Parker, independent treasury consultant and the former group treasurer of private equity and public companies.

The scale of such loss can be significant. Earlier this year, hackers stole $80m from the Bangladesh central bank after fraudsters obtained the bank's credentials. Further transactions were stopped after suspicions were raised by a spelling mistake; the total loss could otherwise have run to as much as $1bn.

For corporate treasurers, it is important to understand the full range of risks and threats – both old and new – and to make sure that appropriate security measures and controls are in place to avoid these risks. While cyberattacks such as the Bangladesh Bank heist attract significant attention, the risk of fraud has been around a long time. Security and controls should cover both internal and external risks, as well as the more mundane issue of payments made in error, at the wrong time or for the wrong amount.

Depending on the nature of the business, companies may also need to address the security of incoming as well as outgoing payments. "For companies in the B2C environment, it is also important to consider the fraud risks associated with collecting money from customers," comments David Stebbings, head of treasury advisory at PwC. "If you want to provide customers with mobile payment options, for example, it's important to understand and address the associated risks."

A further consideration is the risk that staff could be forced to transfer funds under duress. "As we move away from BACS and CHAPS, which can be stopped, to Faster Payments and 24-hour payments, we become more susceptible to this sort of fraud," remarks James Kelly, group treasurer at AB Ports. "Many banks offer a login password, which indicates a payment under duress – but this could escalate a dangerous situation if the funds do not appear to clear for the beneficiary."

IKON IMAGES/PATRICK GEORGE

Taking action

When it comes to tackling these risks, it's important to seek out up-to-date information about the nature of any possible threats. Nicholas Corker, assistant treasurer at Severn Trent, says he engages in regular update meetings with relationship banks in order to understand current threats. "In my recent discussions with banks, they've highlighted how fraud is becoming more sophisticated," he explains. "When I get the information through from banks, I'll forward that to the relevant teams – the risk team, internal audit and accounts payable."

With a clear understanding of the possible threats, it is important to mitigate any risks relevant to the company. From understanding the risks to managing tokens and passwords safely, treasurers should focus on the following areas:

Standardise and automate

When it comes to mitigating payment risks, Corker says the main goal is to standardise processes as far as possible. From an accounts payable point of view, this means making sure that everything goes through recognised procurement processes, such as a three-way match, whereby supplier invoices are matched with the relevant purchase orders and receiving reports.

"If we have to make manual payments, we try and keep those to a minimum, with full segregation of duties in place," he adds. "Internal audit has a rolling cycle of audits, which includes reviewing our controls to make sure they operate effectively. They report up to the audit committee, which reports into the board."

Corker says the company currently operates a manual treasury management system, but that a goal over the coming 12 months is to automate the system so that payments go through an automated, rather than a manual, approvals process.

Watertight

FROM CENTRALISATION TO SEGREGATION OF DUTIES TO KEEPING ABREAST OF THE LATEST FRAUD TECHNIQUES – SECURITY REQUIRES CONSTANT VIGILANCE. REBECCA BRACE INVESTIGATES

Review processes

Bruce Meuli, global business solutions executive, global transaction services, at Bank of America Merrill Lynch, emphasises the importance of regularly reviewing processes from a control and compliance perspective, focusing on root cause analysis of any events, the ability to identify, evaluate and mitigate risks, and the continual education and training of personnel.

Centralise payments

Centralisation strategies can also be a useful tool in strengthening security. "The best practice is to centralise payments through a global payment hub. This means that there is a single centralised system managing all payments, sometimes run through a shared services centre [SSC]," says Bob Stark, VP Strategy at Kyriba. "From a technology perspective, implementing a single conduit to the organisation's banks reduces risks, as well as lowering costs and simplifying the management of payment systems."

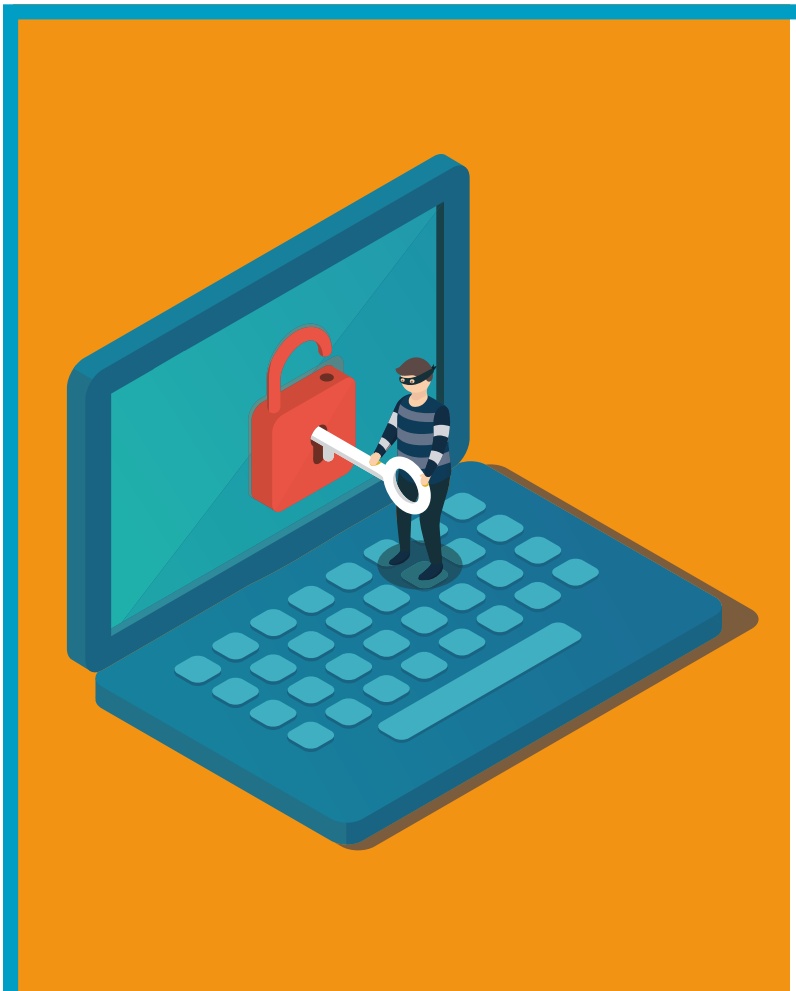
Stark says that having a single payment system makes it easier for CFOs to ensure that the same types of controls are consistently applied to all payment workflows. "Minimising exceptions to payment policies is one of the best ways to achieve payment security," he adds.

However, PwC's Stebbings points out that not all centralised structures are suitable for managing all types of payment risk. "Certainly, you want your high-value payments to go through a centre of excellence so that you can control them better – but the SSC may not necessarily have the specialist resources for that," he observes. "SSCs are often about saving labour costs, which can work for commercial payments where controls are likely to be in the enterprise resource planning – but they may not have the skill set needed for appropriate control over irregular high-value payments."

Have a consistent policy

"All treasuries should have board-approved objectives, policies and procedures," says Parker. "Within those policies and procedures, you should have a control framework that specifies who can do what, what your authorised payment instruments are, what the limits are, who can authorise a certain payment and whether dual authority is required for payments over a certain amount."

Where policy is concerned, Stebbings points out that it is important to have a clear understanding of who is responsible



SHUTTERSTOCK

CEO FRAUD

Also known as business email crime (BEC), CEO fraud is a significant concern for companies around the world.

CEO fraud involves a fraudster sending an email that appears to come from the account of the CEO or CFO of a company. The email asks an employee of the company to make an urgent payment to an overseas bank account, usually citing a confidential project, such as an acquisition. Increasingly, fraudsters are drawing upon personal details to make these emails sound as authentic as possible, and are often sent when the CEO is out of the office. The targeted employee may receive phone calls as well as emails.

The losses resulting from this type of fraud can be enormous. According to data published by the FBI, companies have lost more than $2bn in the past two years as a result of this type of scam. In February, Action Fraud UK revealed that it had received 994 reports of CEO fraud in the past year – including one company that lost £18.5m.

"BEC schemes where CEOs are targeted and mimicked can be avoided through the execution of consistent payment policies and additional mechanisms to confirm identify, including electronic approvals and digital signatures," says Kyriba's Bob Stark. "Also, as these types of stories are publicised, more CFOs and treasurers are able to recognise suspicious behaviour and implement appropriate safeguards."

Rick Martin, treasurer of GasLog, says that the company's IT team weeds out most such attempts before they enter the system. "On the rare occasions that they do, our staff is well-educated in identifying telltale hallmarks of these attempts, and also in both the treasury policy, and the process/approval flow charts that govern all payment processes," he adds. "These are tested regularly by internal audit, and jointly approved by the CEO and CFO. Further protection is provided by strict segregation of duties, and authorisation hierarchies that are embedded in both our enterprise resource planning, and our e-banking platforms."

for payment fraud. "Clearly the treasurer is responsible for treasury payments – but are they also responsible for commercial payments? I suspect that if you were hacked there would be some responsibility there," he says. "So even though this may not be the direct responsibility of the treasurer, you would expect them to be involved with the writing of the policy and making sure that the software vendors they use are following the relevant policies."

It is also important to make sure that any policies in place provide consistency across the organisation. "Having different policies for accounts payable payments versus treasury-initiated payments, and different procedures yet again for special payments, such as M&A, is what creates exceptions that fraudsters prey upon," says Stark. "There must be a payment policy that is implemented by all departments that initiate, approve and remit payments."

Nor is it enough simply having a policy in place. "It must also be understood by the board and operational executives as to how these policies are executed," says Meuli. "Ticking the box with a signed document is not enough. It must be an active document that is reviewed and managed against performance."

Manage passwords and tokens

Rick Martin, treasurer of GasLog, says that the tokens and passwords required for authorisation on the company's e-banking platforms are strictly monitored by the system administrators. "They are also limited in numbers to provide sufficient segregation of duties and redundancy, but no more," he adds.

"The treasurer is responsible for treasury payments – but are they also responsible for commercial payments?"

New technology may be helpful as companies look to establish more secure authentication processes. Shirley Inscoe, senior analyst at Aite Group, says that hardware tokens, issued to cash management customers for many years, can be overcome by some forms of malware. "In addition, hardware tokens may break, be left behind and not available when needed, or have the battery die at an inconvenient time."

However, Inscoe says that newer forms of technology can be used to enhance security – citing the use of biometric data to access accounts, including technology that enables users to register their eye vein patterns, for instance. "This allows customers to use the camera on mobile devices to easily authenticate themselves without being bothered with user names, passwords or tokens."

Consider all threats

While the latest cyberthreats may attract more headlines, it is important to remember that not all payment-related risks are highly sophisticated. Damian Glendinning, treasurer of Lenovo, says that traditional, non-connected payments and cash management processes are far from being completely secure.

"How hard is it to forge a paper signature?" he asks. "How hard is it to intercept and modify a written instruction to a bank, or a paper trade confirmation? How secure are voice systems for placing orders, especially in the FX market? Anyone who thinks these are safe has clearly never listened to the recording of a trade captured on a tape-recording system."

Conclusion

Managing the risk of loss through error or fraud continues to be a top priority for corporate treasurers. While new threats may be arising, the tools that treasurers have long used to manage payment-related risks continue to be relevant – from the segregation of duties to effective policies. That said, treasurers do need to understand the nature of emerging threats, and should explore how new technology solutions can build upon the safety measures already in place.

Rebecca Brace is a freelance journalist specialising in corporate treasury and banking