SIGN & DELIVER

Digital certificates and biometric ID are among the front-line defences against cybercrime on the technological highway. Lesley Meall explains

Risk has always been a big word in the treasury function, but developments in IT are making it into a much bigger word. "The world is changing and the world of treasury is changing, too," says Sebastian di Paola, the partner who leads PwC's global treasury consulting practice. "Some trends in treasury also increase the risk in treasury," he adds, just as some trends in technology also increase the risk in technology.

In recent years, many treasury functions have been working to standardise and streamline the processes in their financial supply chain: centralising cash management and payments, and moving towards end-to-end straight-through processing (STP) – for internal treasury and for relationships with banks, customers and suppliers. But despite the associated benefits, as di Paola points out: "The more integrated your treasury processes are, the more at risk they are from an IT security perspective."

Not that lack of integration is any guarantee of security, of course. Recent EU legislation (2010/45/EU) is designed to encourage electronic invoicing and support STP. But it may actually weaken the security of some electronic invoice (e-invoice) transactions and create barriers to STP, because the directive obliges organisations to accept insecure PDF documents as e-invoices (see www.treasurers.org/node/9453).

Certificates and signatures

Although qualified electronic signatures and secure electronic data interchange are among the various methods the directive allows organisations to use to maintain invoice 'authenticity and integrity', it also allows the use of 'business controls' to ensure a reliable audit trail between invoice and supply. "Unsigned electronic invoices on their own are not secure," says Steve Roylance, business development director with digital certificate authority GlobalSign.

The stance being taken by the EU may be confusing some businesses. "Since the directive was adopted across Europe in January 2013, we have seen new customers adopt electronic signatures and some long-standing customers move away," reports Roylance, perhaps because some organisations believe their business controls and security procedures will suffice. "Time and the potential fines levied by local tax authorities will tell," he adds.

The security of a transaction isn't just about the invoice; it's also about the delivery channel or network behind it. Tom Rahder, vice president of product strategy with the trade finance specialist Bolero, says: "We view digital certificates as having been issued to an entity. It's the organisation's stamp, but a digital signature is only as good as the processes behind it."

Mobile mayhem

Electronic transactions are also creating treasury security challenges a little closer to home, as treasurers increase their use of tablets and smartphones. "This creates lots of privacy and security issues," says Etay Maor, fraud prevention solutions manager at security specialist Trusteer, as many of the tablets and smartphones being used are the personal property of employees.

Treasurers do not typically require 24/7 mobile access to all of the functionality in their systems, but they can benefit from mobile access to some treasury functionality. "Many treasury professionals need timely liquidity information to support decisions and the ability to access that anywhere through a mobile app is useful," says Tim Wheatcroft, director of corporate communications at Kyriba, a cloud treasury management specialist.

A treasury app can enable you to access information such as a cash balance or to forecast and execute tasks such as wire transfers and payment authorisations. But the security of a mobile device is only as good as all of the apps installed on it – and all of the people using it. "Cybercriminals are investing a lot of money in making their malware difficult to detect," says Maor, and corporates need more than secure treasury software to prevent unwanted access to their systems.

When Kyriba Mobile was introduced for use on Apple devices a year ago, access security was a priority: the sign-in requires users to provide a valid user ID and a strong password, as well as an optional second factor of authentication. Apple's new biometric Touch ID has added

If there is a cyber fraud, the treasury function is one of those most likely to be hit, so it is important for treasurers to presume nothing where security is concerned

another security layer. “Anything that can make end-point security more robust is a good thing,” says Wheatcroft, “and fingerprint scanners appear to provide a strong solution in this area.”

Security apps are also emerging that use the camera on a smartphone as a means to provide a biometric identity verification system. EyeVerify, for example, has developed software that identifies you by the pattern of veins in the whites of your eyes, something it claims is as accurate as a fingerprint or iris scan, without requiring any special hardware. Users simply look into the camera lens on a mobile phone and move their eyes from one side to the other.

Sneaky little critters

But cybercriminals exploit a variety of techniques to infiltrate corporate networks. According to Trusteer, compromising an employee end-point device is a far simpler path into the business than a direct attack.

“Malware has lots of layers and it’s getting smarter and more evasive,” says Maor. Once it’s downloaded onto a device, without specialist software it will go undetected, then it will make its way back into the enterprise, where it can gather information such as network credentials – and simple-to-use malware tools are widely and cheaply available online. “It takes just minutes to design malware that anti-virus software will not detect and this can target the treasury office very easily,” says Maor.

If there is a cyber fraud, the treasury function is one of those most likely to be hit, so it is important for treasurers to presume nothing where security is concerned. Yet one recent PwC survey found that 58% of businesses lacked a mobile security strategy, while in another survey by the firm, 74% of C-level executives and IT directors described their security activities as effective despite also admitting to a 25% increase in detected security incidents over the previous year.

“There seems to be a high level of misplaced confidence among senior management,” says di Paola, which could impact negatively on the treasury function. “When the growing risk of cybercrime is layered on top of trends in treasury and developments in technology, it creates a whole new world of threats,” he adds. So treasurers need to ensure that their business process knowledge and the cybersecurity knowledge in IT both inform security strategy.

“Treasurers need to concern themselves with the IT side of risk, just as much as the IT team does,” says Wheatcroft, whether they are directly or indirectly responsible for risk management. “If the treasury system is compromised in any way, it is treasury who will feel the most pain.”

Lesley Meall is a freelance journalist specialising in finance and technology

FUTURE SHOCK

As science fiction increasingly becomes science fact, treasurers can look forward to even greater security threats – and you may need more than a biometric scanner to protect your systems and your secrets from them. In the future, some of your biggest security problems may be caused by the smallest devices.

Researchers have already developed tiny computers just one cubic millimetre in size – nicknamed ‘smart dust’ – that work just like their larger ancestors. The University of Michigan, for example, has built working prototypes dubbed ‘Michigan Micro Motes’, which use sensors to collect data and then transmit it via radio waves.

It’s only a matter of time before devices such as this can scavenge power from their surroundings effectively enough to make them commercially viable. This will make traditional notions of privacy and security redundant, and make today’s security challenges seem like a walk in the park.