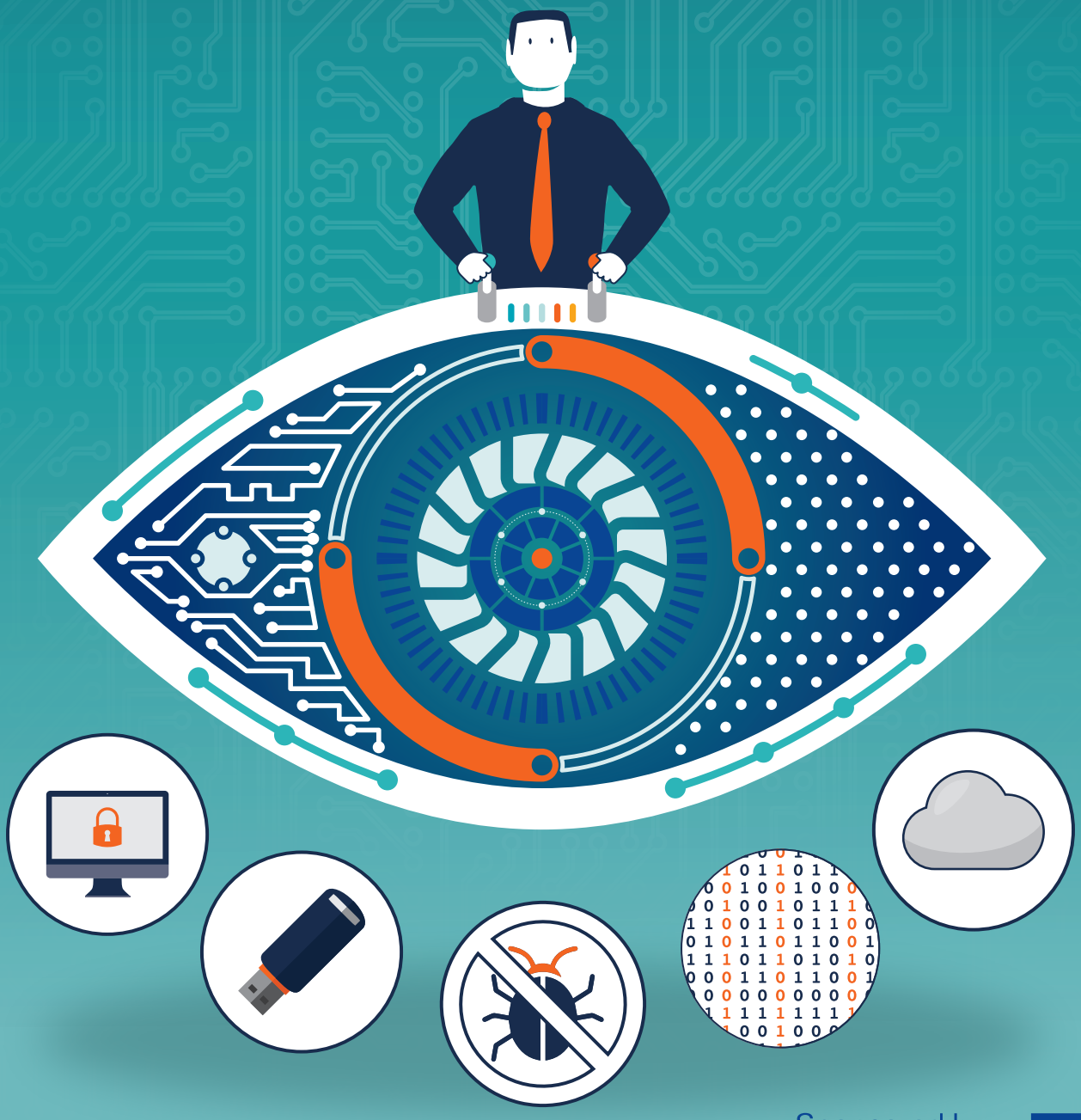
The Economist Intelligence Unit

THIRD-PARTY RISKS:
The cyber dimension



Sponsored by Deutsche Bank

CONTENTS

ABOUT THIS RESEARCH

In April-May 2017 The Economist Intelligence Unit (EIU), on behalf of Deutsche Bank, surveyed 300 senior corporate treasury executives to find out how they are preparing themselves for current and future third-party cyber-related risks and opportunities.

Executives were drawn from 19 different sectors, including aerospace/defence, agriculture and agribusiness, automotive, chemicals, construction and real estate, consumer goods, education, energy and natural resources, entertainment, media and publishing, financial services, government/public sector, healthcare, pharmaceuticals and biotechnology, IT and technology, logistics and distribution, manufacturing, professional services, retailing, telecommunications, transport, travel and tourism.

In addition, we conducted a series of in-depth interviews in June-July 2017 with senior treasury executives from around the globe. Our thanks are due to the following for their time and insight (listed alphabetically):

- Ok Azie, vice president and treasurer, Baker Hughes
- Catherine Fields, assistant treasurer and director of global risk management, Hitachi Data Systems
- Yves Gimbert, group treasurer, ENGIE
- Gerrit-Willem Gramser, group treasurer, Akzo Nobel
- Aashish Pitale, group treasurer, Essar

The Economist Intelligence Unit bears sole responsibility for the content of this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor. This report was edited by Renée Friedman.

EXECUTIVE SUMMARY

Corporate treasury is now a top target for cyber-criminals. 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.

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 potential losses are huge. Hackers infiltrating individual companies have stolen tens of millions of dollars in a single attack. The stock price of breached companies falls and CEOs are sacked. Data losses create reputational damage and lawsuits from inside and outside the company. Even mergers and acquisitions can be derailed or altered in value to the tune of hundreds of millions of dollars, as in the case of telco Verizon's acquisition of internet company Yahoo!

Evidently, cyber-security is not an issue that treasurers can ignore. This report, written by The Economist Intelligence Unit (EIU) and sponsored by Deutsche Bank, investigates the state of treasury cyber-security and identifies what needs to be done to improve it.

Key findings

Our research found that most treasurers believe their companies are doing well at implementing basic security measures. They have moved aggressively to strengthen their cyber-defences by initiating penetration testing to check for internal and external vulnerabilities, updating software systems to evade new lines of attack, and taking steps to limit company network and data access to both employees and third parties. Companies are also training employees on fraud.

However, our research also found serious gaps in corporate defence, including vulnerabilities hidden within third parties and their subcontractors. Indeed, a significant minority of respondent companies are missing some basic security precautions.

Nineteen percent of companies do not check whether their suppliers use the same methods for identity authentication as they do. This leaves an open door for fraud.

According to 18% of companies surveyed, only a minority of clients and suppliers follow the same or similar regulatory and compliance rules as they do.

Because 14% of companies do not insist that information security requirements which

currently apply to third parties also be extended to their subcontractors, they are giving cyber-criminals the opportunity to steal data.

Internal penetration testing is performed by 92% of companies. However, 33% do *not* conduct external testing, leaving a worrisome gap that can be exploited.

Only 38% of companies require all of their third parties and suppliers to perform penetration testing. This may be risky, given the increasing number of data and other network security breaches that have been reported.

But while treasurers need to be intimately concerned with cyber-security, ensuring technical security is not their responsibility. This report nevertheless identifies some measures which treasury departments can adopt to ensure that the assets they protect are effectively secured.

CHAPTER 1: WHY TREASURY IS A TARGET

Cyber-criminals target corporate treasury for a simple reason: it's where the money is. Hacking treasury is one of only a few ways to steal very large amounts of money very quickly. And unlike data theft or even ransomware, which can cause damage and cost over time, treasury hacks can cause immediate, significant and usually irreversible financial loss.

Hackers are also aware that many companies still do not take cyber-security seriously. In February 2017 consultancy Deloitte found that only 5% of FTSE 100 companies disclosed having a director responsible for cyber risks.[1] This suggests a worrying misalignment with internal priorities, given that 71% of corporations identified IT systems failure among their principal concerns, and 72% highlighted a cyber-attack as a risk.

Institutional investors are also increasingly worried about board commitment to cyber-security. Legal and General Investment Management (LGIM), an asset management firm, calls for compulsory cyber-audits.[2] "Cyber-security is a significant risk to our investee companies," warns David Patt, senior analyst for corporate governance and public policy at LGIM. "We are concerned that many responses we receive to this major corporate risk are insufficient. Boards need to be more aware of their operational environment and emerging threats to their business. Simply put, it can affect a company's value."

Few firms are making the necessary investment: staffing levels and the seniority of chief information security officers (CISOs) remain low. In most firms cyber-security is a nascent competence with responsibilities spread over IT, business continuity, internal audit and possibly a separate enterprise resource planning (ERP) team.

Certain factors make managing cyber-security especially difficult for treasurers. They are neither fully responsible for ensuring that their departments cannot be compromised nor completely in control of the systems, people and processes that lead to compromise.

Most treasuries are still to some extent decentralised, especially in their emerging-market operations. This has allowed hackers to exploit local teams and systemic fragmentation. In its *Global Treasury Benchmark 2017 Survey*,[3] consultancy PwC found that 67% of people involved in treasury processes do not report directly to the treasurer—such is the level of outsourcing and the use of shared service centres (SSCs) in treasury.

According to Gerrit-Willem Gramser, group treasurer at Dutch chemicals company Akzo Nobel, "in general the most dangerous [problems] are localised operations, where staff has too many roles which they carry out by themselves with no real checks or have local tools. Sometimes the local tools themselves don't have interfaces which are sufficiently protected. We have mitigated that risk by deploying a central process and only using SWIFT for our bank connectivity."

[1] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-governance-in-focus-cyber-risk-reporting.pdf

[2] https://uk.reuters.com/article/uk-legal-general-cybersecurity-audit-idUKKBN0TJ0TS20151130

[3] https://www.pwc.com/gx/en/services/audit-assurance/corporate-treasury-solutions/publications/corporate-treasury-benchmarking-survey.html

Aashish Pitale, group treasurer at Indian industrial giant Essar Group, relies on international vendors because, he says, "they will use the same systems globally, so I trust their systems are prepared for cyber risks." He believes that these international vendors have stronger cyber-security and strengthen his own systems in terms of security robustness.

Treasury is an attractive target for other reasons. It is a relatively junior, non-C-suite function in many organisations, and some of the most spectacular business email compromise (BEC) scams have involved fake instructions from the CEO to treasury staff, ordering them to make secret payments linked to deals that must not be disclosed to staff below board level. In hindsight, it can seem incredible that these payments were made, but the fact that they were exposes the huge cyber risks many companies are running as a result of the way in which their treasuries operate.

Finally, treasury is all about connectivity. It is a gateway into other core corporate management information systems. If administrator rights in a treasury system can be hijacked in one place, then it may be possible to access global ERP systems, global HR systems, regional SSCs, payment factories and other key databases.

The criminals have figured all this out. Through extended reconnaissance they have discovered that treasury remains badly protected because it often relies on systems that were designed long before cybercrime was envisaged. Untrained treasury staff and lethargic systems enable these criminals who face almost no prospect of capture and spend only pennies to execute their attacks.

This has led to an explosion of treasury-targeted phishing, email-delivered ransomware and BEC scams: they are cheap, scalable and offer extremely high returns. Ransomware cyber-criminals took in about US$1bn in 2016, based on money coming into ransomware-related Bitcoin wallets.[4] According to FBI data, between 2013 and December 2016 cyber-criminals stole US$5,302,890,448 in 40,203 cases from US and international businesses.[5]

The top treasury scams

The simplest scams are invoicing frauds. Once systems have been hacked to discover who makes payments and how, they can easily send false invoices from invented suppliers to the right person in accounts payable and then harass them into paying them.

They can mount man-in-the-middle (MIM) attacks, in which they intercept real buyer/supplier communications and send their own versions of invoices or payment instructions, spoofing the email address of the company owed the money, adding their own bank details. This way, the buyer thinks they are sending their payment to the supplier, but they are really sending it to a hacker.

In June 2015 Europol, the law enforcement agency of the EU, announced that it had dismantled a group of cyber-criminals active in Italy, Spain, Poland, the UK, Belgium and

[4] https://www.ic3.gov/media/2017/170504.aspx

[5] http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html

Georgia, who used MIM fraud to steal €6m (US$7m), accumulated within a very short time.

Another approach is to deliver ransomware which, if activated, can encrypt and delete core data or disable key treasury or ERP systems. The criminals then demand money to decrypt the data.

Business email compromise

Perhaps most spectacularly, criminals may hack into email and other systems to build up a detailed picture of staff and company operations. They then create email sequences that include confidential company information and which appear to come from senior management. Generally these take the form of urgent requests to transfer money.

These attacks, known as BEC scams or CEO fraud, differ from spam-based malware attacks, which generally carry ransomware. They use social engineering and inside information gathered through reconnaissance to target specific individuals with customised, believable (but fake) emails. This is also known as spear-phishing.

BEC fraud has claimed a number of high-profile victims. On August 16th 2016 Leoni, one of the world's leading wire and cable manufacturers, announced a loss amounting to approximately €40m owing to a case of BEC fraud.

The finance department of Leoni's factory in Bistrita, Romania, received several emails purportedly from one of the company's senior German executives. Using inside information to appear convincing, the criminals convinced the recipient that it was a genuine request, and a series of cross-border payments totalling €40m were made. At the time, email confirmation for payments was an accepted procedure at the firm's Romanian unit.

In an investor presentation later that year Leoni disclosed that what they called the "CEO fraud" had used falsified documents and identities as well as electronic communication channels and involved rule infringements by some staff. In mitigation, the company now checks payment transactions more stringently and has introduced additional controls and staff training. It has also instigated both internal and external reviews of its internal control system (ICS), its IT security, its risk-management system and the internal audit department.

In early 2016 Fischer Advanced Composite Components AG (FACC), an Austrian aeronautics company, announced that it had also fallen victim to a BEC scheme that netted €42m through a spear-phishing attack. The attack used a fake email which impersonated the then CEO, Walter Stephan, conning one of FACC's finance staff into wiring money that was supposedly for one of the company's acquisition projects.

In its 2015-16 financial report FACC disclosed that although it was able to stop the transfer of €10.9m, "it is expected that the amounts frozen in receiving accounts will

not be reimbursed in the short term". In addition, "the loss incurred by the company as a result of the cyber fraud also led to an outflow of liquid funds totalling €52.8m and left FACC with an operating loss of €23.4m".

Data, as well as money, are a target for criminals. In February 2016 social video app Snapchat issued a blog apologising to its staff after a spear-phishing attack had tricked an HR employee into handing over payroll information about "some current and former employees".

This fraud demonstrates that seemingly innocuous requests for data can result in significant damage. In addition, with new regulations, in particular the EU's General Data Protection Regulation (GDPR), which enters into force in May 2018, data privacy will be backed up with fines of up to 4% of a company's global turnover. That email of employee tax details could have cost the company a great deal of money. Treasury, and every other department, need to understand the wider context.

CHAPTER 2: THE VULNERABILITIES OF TREASURY

The technical vulnerabilities which cyber-criminals exploit in their hacks are not unique to treasury departments, but certain characteristics make treasuries especially prone. For example, a core treasury objective is global connectivity, as it enables improvements in visibility and efficiency. Siloed systems are of limited use; interconnected systems are more likely to allow hackers in.

"IT environments within companies are changing all the time. And with all that continuous change in every area, I think we can just see how a small oversight can easily be created," explains Mr Gramser of Akzo Nobel. "As soon as you have an oversight, you have a weakness, and a weakness can be penetrated. The connectivity between the different systems is typically the weakest link."

More generally, treasury is technology-heavy but sits outside the IT department. Challenged by regulatory change and increasing complexity brought about by cross-border growth, new regulations and staff reductions, treasury has turned to technology to solve its problems and deliver the efficiencies companies now demand. Treasurers can seem more the managers of endlessly iterating IT projects than finance staff.

The Economist Intelligence Unit's report *Managing risk in challenging economic times*, published in 2016, found that almost seven out of ten survey respondents were increasingly concerned about external technological risks, such as cyber-attacks. However, closer co-ordination between IT and treasury still does not seem to have progressed.

Outsourcing and control issues

Treasury security is also jeopardised by organisational distribution. "Already two-thirds of staff involved in treasury processes are not reporting directly or even indirectly to the treasurer", according to a 2017 survey by PwC.[6] "A number of treasurers have outsourced their back office and payment factory processes to shared services and exposure reporting increasingly involves local finance."

This is an environment in which technology is being repeatedly adopted and changed both inside and outside treasury. Treasury data and processes are being moved into external SSCs and onto cloud-based systems; they sit in treasury management systems (TMSs), which were not designed with security in mind and which are often not updated or patched to the latest version; and data are exchanged with ERP systems which suffer from the same issues, even when they are cutting-edge.

Cyber-criminals have noticed. As well as core treasury processes such as payments, they are increasingly targeting ERP systems. Not only are these interesting targets in their own right, given the data they pull together, but they are also potential conduits into other, critical business software.

[6] https://www.pwc.com/gx/en/services/audit-assurance/corporate-treasury-solutions/publications/corporate-treasury-benchmarking-survey.html

The potential impact of an ERP compromise will vary depending on the user, the ERP implementation and the cyber-security infrastructure the company has in place. But one company has estimated that an ERP outage could cost US$22m per minute.[7] This figure reflects the fact that large companies don't just run one instance of their ERP software and that so many other business-critical systems rely on ERP systems. This outage cost does not include the costs of exfiltrated data or the reputational risk of a breach.

Third-party security

Treasury can also be hacked via third-party relationships. The now infamous Bangladesh Bank heist, which used a combination of techniques to steal US$81m from the country's central bank, illustrates that not even core payment systems are 100% secure and can be used to commit fraud. In a blog post outlining the details of the hack, cyber-security services provider BAE Systems concluded: "All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed."[8] The same advice holds true for corporate treasury.

One might assume that banks have a high level of security, but it is not enough to assume. Mr Pitale of Essar Group believes that one of the necessary items for his treasury is having a dealing trail. All lines are registered with the bank so that they know they are only dealing with him, and cross-verification takes place on a different line to ensure the data are correct.

Treasury departments must ask their bank questions about security and the money-management systems as well as the portals they use. Key questions include: Do they use a secure email system to protect confidential communications? Do they employ strong/two-factor customer authentication? Do they offer the ability to check the IP address of logins and match them with pre-assigned customer addresses? And do they look for unusual patterns of behaviour in customer accounts? If not, then they are insecure at a fundamental level.

[7] https://www.onapsis.com/onapsis-discovers-and-helps-mitigate-new-critical-cyber-security-vulnerabilities-affecting-all-sap

[8] http://baesystemsai.blogspot.co.uk/2016/04/two-bytes-to-951m.html

CHAPTER 3: THE TREASURY RESPONSE

Our survey reveals that some cyber-security measures are now practically universal. Over the past 12 months, for example, 93% of respondent companies have taken steps to improve employee access controls on confidential company information and documentation. And 96% of the companies surveyed say they have an in-house process to limit third-party access.

But as these examples demonstrate, a company's IT environment is only as secure as its weakest point, and our survey suggests that many companies are not being as vigilant as required.

The risk posed by insecure third parties, which hackers can use as conduits into their target organisation, is widely recognised. In many cases, this lesson has been hard won. "We are all interconnected—suppliers, customers, subcontractors or manual payments processor," says Yves Gimbert, group treasurer of French utility company ENGIE. "I would say we all face the consequences of the theory that we are all only as strong as the weakest link. And the weakest link will be the one with a low corporate culture of protection."

Chart 1

Third-party authentication: the sectors with the lowest percentage of authentication testing
(% respondents)

Source: The Economist Intelligence Unit.

The share of companies actively bringing third parties into compliance with their own standards ranges from 81% to 94% on several measures. But there are still open targets: 19% of companies do not check to see if their suppliers use the same authentication strategy, which may conceal a gap in security protection by third parties.

According to Catherine Fields, assistant treasurer and director of global risk management at Hitachi Data Systems, companies need to understand who every supplier is and think exhaustively about their contribution to the company's security posture. She gives the example of a vending machine company. Typically, there would be no reason to check their authentication processes. However, if the vending machine

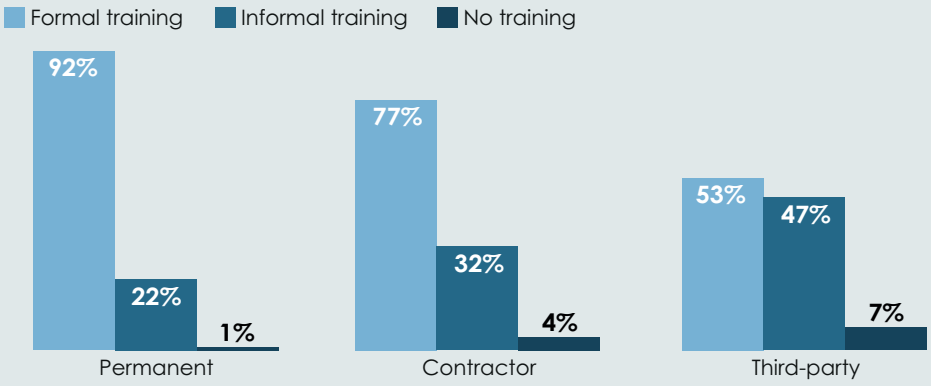
Training and education

Technical controls are vital, but employees are increasingly targeted as potential weak points. Treasurers are no exception. Ok Azie, vice president and treasurer at oil and gas services provider Baker Hughes, was sent a fake email purporting to be from the company's chief executive officer, asking him to transfer money for a specific transaction.

It was obviously a scam to Mr Azie. "[The CEO] doesn't ask me to move money," he explains. But the example underscores the need for employee training and education—at every level of the organisation.

Chart 2

Employees by type receiving training by type on access to company network server segments
(% respondents)



Source: The Economist Intelligence Unit.

According to the treasurers surveyed, companies are doing a good job in terms of training. For example, 92% require formal training of permanent employees concerning the extent of access to company network server segments.

Mr Gimbert of ENGIE notes that his company expanded its security procedures three years ago, and today its training is co-ordinated between corporate treasury and corporate IT security. This training includes cyber-security, phishing and malware. The training focuses on treasury fraud, payment fraud and fraudulent attempts from people posing as the company CEO or third parties receiving payments from the company. "As threats constantly evolve, these training programmes must be repeated on a regular basis," he says.

Blind spots remain across the companies surveyed, however, especially with respect to third parties. Nearly 48% of respondents say their third-party vendors provide informal employee training on cyber risks associated with the company for which they are working, while 7% provide no employee training, either formal or informal.

Working with IT

Perhaps the most important measure that treasurers can take is to maintain a healthy collaboration with their IT and cyber-security teams. At ENGIE, the treasury is involved in securing the company's customer database, which contains records of some 15m individuals, and its ability to collaborate with IT is essential, explains Mr Gimbert. "We work hand in hand with the IT department as the company moves more data and more functions to cloud-based solutions. Every new change that involves fraud or cyber risk is audited and tested by the company's IT function working in conjunction with the treasury team."

This need for collaboration is echoed by Mr Pitale of Essar Group. He has mandated that an IT employee is physically located within the treasury department.

But the ability and inclination among treasurers to work with IT vary hugely. Ms Fields is assistant treasurer at Hitachi Data Systems, but her role extends well beyond her immediate department. "I am also our director of global risk management, which means I also handle insurance," she explains. As a result, she is deeply involved in cyber-security. "I have a very broad-reaching perspective when it comes to cyber because I am also responsible for making sure that I am comfortable with the level of coverage that we have with respect to cyber-insurance. This means that I am working very closely with IT on security issues."

By contrast, another treasurer, who wished to remain anonymous, admitted that he did not even know whether his firm had a business continuity plan or incident response plan in place for a data breach. This same treasurer, asked whether he had direct "conversations with the IT security team about phishing and the potential threat to bank account data," replied: "No, we cannot do that."

This organisational division is definitely a security concern for the company in question.

External validation

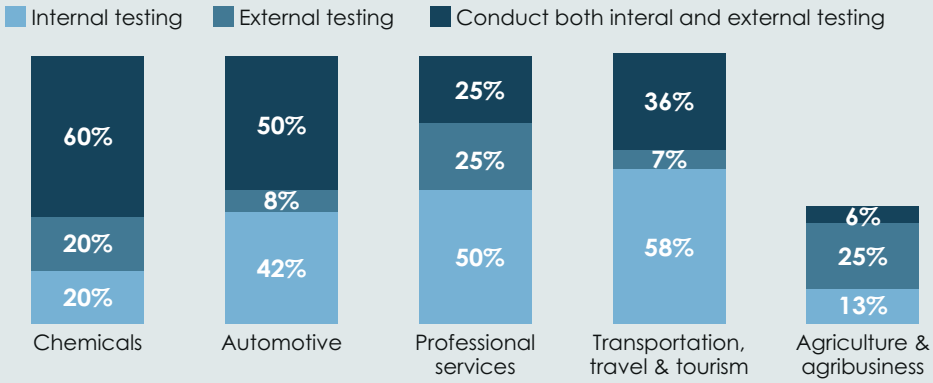
One of the ways in which treasury can co-operate with IT is in designing external tests of their systems. Penetration (pen) testing is a common, basic technique in which experts are hired to attack company systems from the inside and the outside to reveal weaknesses.

Significantly, 33% of all companies do not conduct external pen testing. "This is where corporates are probably falling a bit short," says Ms Fields. "We tend to be more reactive and defensive as opposed to getting out there working with our business partners as we should, especially with anyone who has access to our network."

All survey respondents report that their company has conducted some type of pen testing, either internal only, external only or both internal and external. However, only

Chart 3

Sector variations in penetration testing regime
(% respondents)



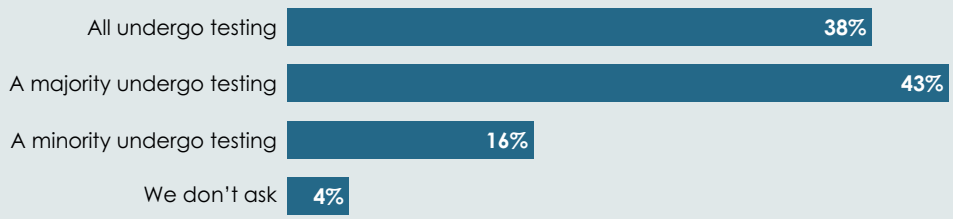
Source: The Economist Intelligence Unit.

59% report that their companies have carried out both types of penetration testing. The remaining firms are leaving themselves needlessly vulnerable.

To address this matter, Hitachi Data Systems has stepped up mutual efforts with third parties to make sure that the right security measures are in place. Last year the company hired its first CISO to oversee this effort to enhance security protection with third parties.

Chart 4

Penetration testing by third parties
(% of companies requiring pen testing by third parties)



Source: The Economist Intelligence Unit.

Industry variation

Our survey also reveals substantial variance in the apparent sophistication of various industries. While highly regulated industries are tackling cyber-security head-on, many companies outside these sectors are not taking it as seriously as they should.

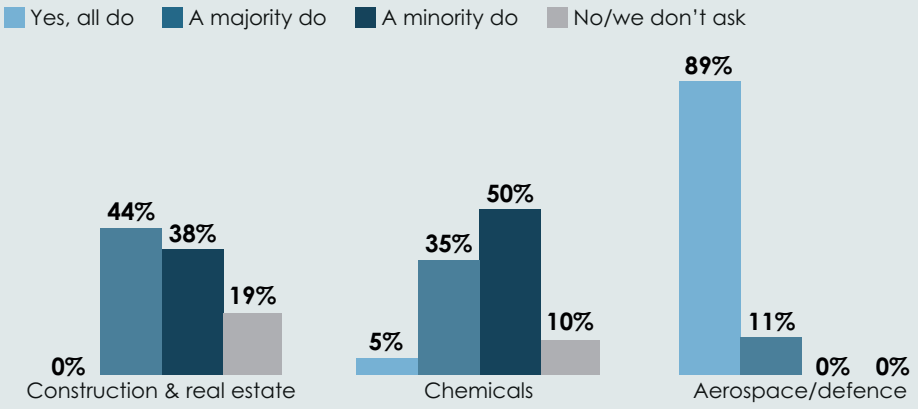
Only 44% of respondents in the construction and real estate industry say that a majority of their suppliers do penetration testing. In the chemicals sector, 35% say a majority do. By contrast, 89% of aerospace/defence sector companies report that all their third parties and suppliers conduct penetration testing.

The survey also indicates that industries which are traditionally less digitised are also less sophisticated when it comes to cyber-security. Repeat outliers in our survey are the construction, manufacturing and agricultural sectors. This may be because they have fewer digital assets to attack and more physical assets to focus on, but their treasury assets are no less worthy of protection.

Furthermore, the increasing network connectivity of physical equipment and infrastructure—the so-called industrial internet—means that these industries may soon be as digitised as any other. Treasurers in such industries would be advised to ensure that their cyber-security foundations are in place sooner rather than later.

Chart 5

Sector variations in requiring third-party penetration testing
(% respondents)



Source: The Economist Intelligence Unit.

CONCLUSION

A new generation of organised, sophisticated and economically driven cyber-criminals has identified corporate payment processes as a source of low-risk profit. Treasurers may own these processes, but they have a limited ability to counter cyber threats directly. So what can treasurers do to ensure that treasury is not the cause of the next big cyber loss? There are key areas for improvement.

Create a security programme

If cyber-security is an objective, then it needs to be defined and measured. Treasury must have its own security management programme, preferably developed in tandem with the company's overall cyber-security strategy. This should recognise that there are at least five sets of people and processes which interact with treasury and which can introduce insecurity:

- Corporate treasury, vendor and employee payment teams;
- Banks which process the payments and provide electronic banking platforms;
- SWIFT and SWIFT bureaus which may provide bank connectivity solutions;
- BACS, EBICS, NACHA and other ACH bureaus and third parties which may provide payment solutions;
- Credit card processing providers.

Basic process improvements

In terms of overall treasury processes, core security relies on a small number of critical measures:

- Centralise system access. Control and secure that access through strong authentication. This is largely a central IT task, but treasury should ensure that its needs are fully represented in the process and that IT understands treasury-specific security measures such as SWIFT's 3SKey;
- Make cash visible: fraud prevention relies on accurate knowledge of what money should be where, and when;
- Disable removable media connections on treasury hardware;
- Disallow bring-your-own-device and the use of social media by treasury staff on treasury hardware.

Securing pay-to-procure

Perhaps most important, treasurers must ensure that control of the procurement process takes cyber-security into account and that their area of the payment workflow is secure. This requires the following measures:

- Ensure that the division of responsibility between treasury and procurement regarding authentication and data protection is clear;
- Secure banking information and interfaces. For example, access to vendor master data should be highly restricted;
- Ensure payment approval rights are clear, appropriately restrictive and regularly audited, and reconcile all payments daily to spot any irregularities immediately;
- Use SWIFT and XML to make payments;
- Isolate the treasury workstation from employee devices and other potential threat sources.

The human factor

Employees should be the key security concern for any organisation. As discussed, regular and relevant education is a must, but companies must also be mindful of the threat posed by malicious insiders. Measures for treasurers to consider include:

- Identify staff whose behaviour is suspicious or has changed recently;
- Mitigate the factors that may prompt an insider threat. What might motivate an employee to steal from their employer, and how can it be addressed?
- Consider the use of external behavioural science consultants to review the potential for insider dissatisfaction and threat;
- Look at systems and processes not simply from the perspective of their resilience to a determined external attacker, but also to an insider who has the correct authorisation and access to core systems but whose aim is theft or destruction of data.

Culture shift

Cyber-security requires a change of culture. Companies are designed to compete with each other for customers and profits. In general, neither they nor their staff are equipped to defend themselves against hostile, criminal attackers intent on intrusion, deception and theft. Knowing about and recognising the tell-tale signs of fraud is one thing, but maintaining the correct level of scrutiny of people and processes can lead to the perception of a Big Brother environment. A balance has to be struck between a level of monitoring that interferes significantly with the day-to-day running of the department and an overly lax security environment that invites cyber-criminals.

Treasury is a target. It's time for treasurers to step up to the challenge.

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: americas@eiu.com

HONG KONG
1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: asia@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com

DUBAI
Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
E-mail: dubai@eiu.com