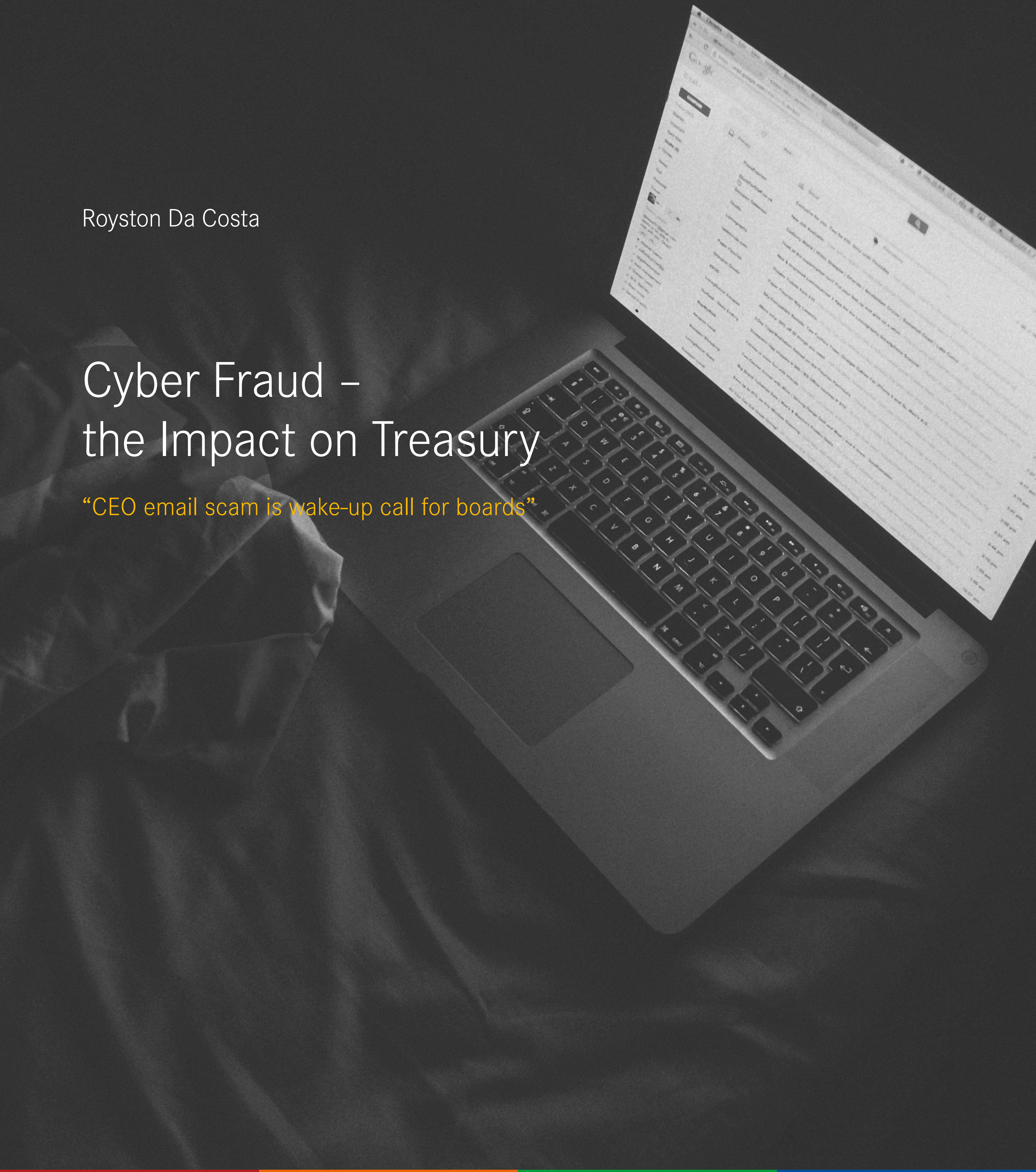
Royston Da Costa

# Cyber Fraud – the Impact on Treasury

“CEO email scam is wake-up call for boards”



# INDEX

Companies should educate their employees in risk management. Employees can be their greatest asset in preventing fraud both internal and external. They can also be their weakest link or greatest risk.

Most companies today recognise they have to tackle the issue of Cyber Fraud. Typically, they will conduct a thorough review of their internal and external processes, e.g. bank payments, data security etc. to ensure they are robust enough and compliant with best practice or the appropriate regulation.

Even though we work in a digital age, communication is still a vital tool that Treasury departments should use to combat some of the scams perpetrated today. Unfortunately, this is often neglected, as indicated by the types of scams that have resulted in financial loss for companies.

There are six areas in relation to Cyber Fraud that I have covered in the article below.

- Financial losses
- Reputation losses
- Staff morale
- Cyber Fraud examples
- Preventative actions
- Cyber Fraud response

# FINANCIAL LOSSES

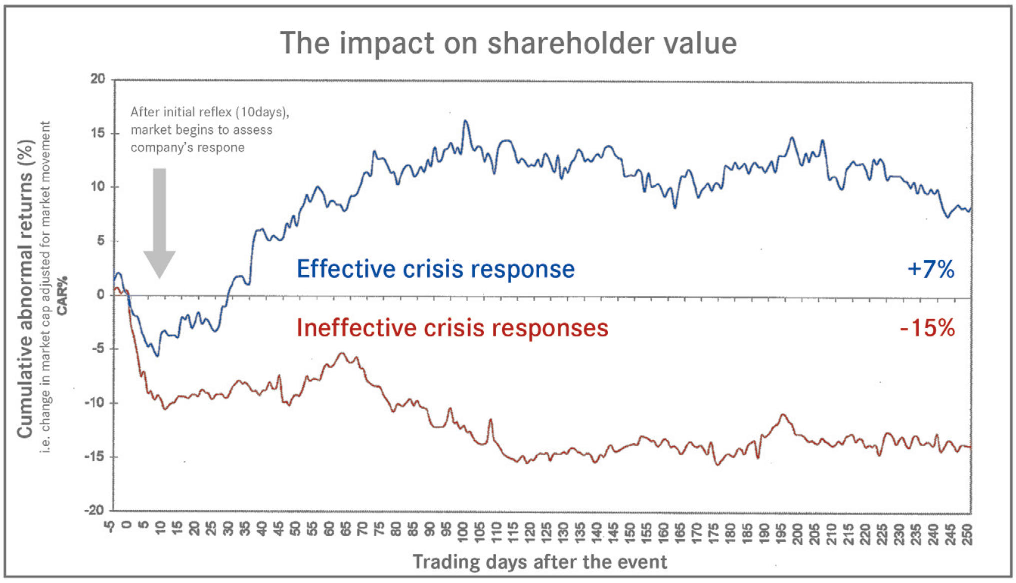
The financial losses of a Cyber Fraud event are determined by several factors. Most notably, how alert the victim is, the level of money or material the victim is responsible for, and the time until the fraud is detected. In addition to the losses incurred directly from the fraud, further losses may occur if the investigation and resolution of the incident prevent normal business operations.

Company operations may be further disrupted if it is required to review the existing processes, and strengthen or introduce new business processes to prevent future Cyber Fraud. Training may be required for existing staff on the new procedures and new systems may need to be implemented.

Furthermore, customers and business partners may feel that a company that falls victim to a Cyber Fraud incident is no longer safe to engage in business transactions. This perception may lead to a direct decline in sales.

# REPUTATION LOSSES

A company’s reputation is at risk whenever a successful fraudulent attack on its systems (or payment processes) is committed. The speed at which the company is able to respond and recover from an attack is critical (see graph below).



Source: `The Impact of Catastrophes on Shareholders Value´, Rory F. Knight & Deborah J. Pretty, Templeton College, University of Oxford

The rate of detection and recovery is also indicative of how robust the processes and financial controls are. This is especially important for publicly-traded companies, where investor perception is essential to acquiring and retaining shareholders.

# STAFF MORALE

Beyond the losses to the company, there are also human impacts to Cyber Fraud for employees. No one wants to be the victim of fraud. Once it happens, it can be quite embarrassing, especially in front of your peers.

It’s easy for a fraud investigation to turn into a “witch hunt” to identify who or what was at fault. Many people will blame themselves for falling for such an ‘obvious’ scam, assuming it was their fault in hindsight.

This is wrong, as no one should be put in the position of being able to process a payment on their own. The process should be robust enough that no one individual has the authority to make a payment on their own, unless unavoidable by law.

In some cases, the fraud may impact the team’s reputation or even compensation. This may result in a backlash towards the team member involved in the fraud, even if they were an innocent participant.

The staff member that was involved may have felt that they had no one to ask and completed the task on a ‘best endeavours’ basis.  They may even suffer an impact to their health, as a result of the fraud.

It should always be the process that is at fault, unless an individual deliberately circumvents the controls in place.

# COMMON CYBER FRAUD RISKS AND SCAMS

The following are examples and explanations of the common risks and scams used by criminals to engage in Cyber Fraud.  It's important to be able to recognise them and avoid falling victim.

## Phishing

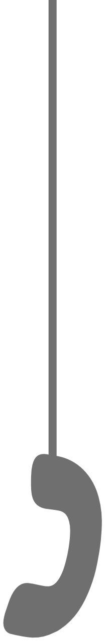
This is the most common type of scam. Emails are sent by fraudsters masquerading as your bank or other trusted organisations to obtain confidential information such as personal information, bank details or passwords. The email will usually contain a link to a fake website, which looks almost identical to the legitimate one. Alternatively, the link may be contained within an attachment to the email. A message usually suggests that you need to act urgently, for example to prevent your online access from being blocked.

Most experts recommend:

- Never click on links in emails that appear to be from your bank.  Go to the bank site directly from your saved favourites link or enter the web address directly in the browser.

Lloyds Bank also suggests the following:

- Be suspicious of emails that are poorly worded or badly spelt. A genuine bank email will usually address you by your name and contain other references specific to you.
- Legitimate bank emails will never ask for your passwords or card and reader codes or lead you to a screen which asks for this information.



## Vishing (Voice Phishing)

These are telephone scams perpetrated by criminals, usually to obtain online banking passwords, confidential details, or persuade you to move money.

Fraudsters, for example, will call you to report a problem with your bank account, and ask you to call back on an official number, say from your bank statement. By holding the phone line open until you call back, they convince you that you've reached the bank. They'll usually ask you to transfer funds to a 'safe' account under their control.

The advice offered by the "Get Safe Online" site (https://www.getsafeonline.org/) is that you contact your bank on a different telephone line to verify the instructions you received.

Lloyds Bank also provides the advice below (further information available on their website www.lloydsbank.com/business/security.asp):

If you're not absolutely certain it's the bank telephoning you:

- Always call them back and use a number you know is correct for the Bank.
- Make sure the phone line is clear before you call by waiting five minutes or use a different line if you have one. Don't rely on your phone's incoming caller display to identify anyone. Fraudsters can make your phone's display show a genuine bank number.
- NEVER divulge full online banking passwords or card and reader codes to anyone on the phone and never move your money out of your account unless you yourself want to pay someone else.

## Spoofing

While not an actual scam, this is a technique used by fraudsters to imitate genuine telephone numbers and email addresses. This can allow them to alter the incoming number on your phone's caller display to one which you know is the genuine number for the bank. Alternatively, they could send an email that appears to come from a senior person within the business, instructing an urgent payment to be made, usually via online banking companies that do not have a process that prevents one individual from processing and approving a payment.

Companies should create an environment where the individuals processing and/or authorising payments actively question what they are doing. They should feel completely comfortable to check with another colleague if they are uncertain about anything to do with the payment.

The advice from Lloyds Bank is:

- Ensure all employees involved in the processing of one-off payments and regular invoices are aware of the potential scams.
- Have a documented process that ensures all new payments or changes to existing payment details are independently verified to ensure the request is genuine.
- If there is any concern that the request is genuine contact the purported sender via a new email (not a reply) or call them directly (using a number from the internal phone directory) to verify.

## The Fraudulent Invoice scam

This form of scam involves fraudsters convincing company employees to change the payment information of a supplier. An example of the scam follows:

The company regularly purchases services from their supplier ABC Consulting.
A fraudster sends a letter to the Company on what appears to be official ABC Consulting headed paper. It states that ABC has changed their bank account, quoting a new sort code and account number for all future payments to be sent to.
The company amends the ABC account details in their payment records held with their bank or internal Accounts Payable (AP) system. When ABC sends the next monthly invoice of £60,000 for services supplied, the Company instructs their bank to send the payment.
The £60,000 is sent to the new account controlled by the fraudster. ABC later contacts the company for non-payment, at which time the fraud is discovered and the funds are long gone.

It is recommended that any change in a supplier's bank account details is independently validated, preferably by someone not in the same department. Furthermore, care must be taken not to use the contact details on the invoice presented as this could be part of the scam. It is best to refer to an internet search engine or Companies House.

## The Fraudulent Invoice scam part II

This form of scam involves fraudsters convincing a company employee to send payment to an unauthorised party. An example of the scam follows:

You receive an email appearing to be from the CFO or other high ranking officer in your company with an attached invoice.  The email claims that the invoice is overdue and must be paid immediately.  You are requested to wire the money immediately to the bank account referenced on the invoice.

Don’t open the attachment!  Management would not request a payment without linkage to an existing invoice in the system.  The attachment is either a complete fake, with fraudulent bank account information, or the attachment could contain a computer virus that could infect your computer and allow the criminal to steal your banking passwords.

## The Cheque Overpayment scam

This form of scam involves fraudsters overpaying an order using a fraudulent check and convincing a company employee to refund the overage to their bank account. An example of the scam follows:

The company receives an order for £2,000 worth of goods from a new client. The client promises to send an online payment so the goods can be dispatched. When the company checks their bank account they find a payment for £62,000. They contact the client who says the overpayment is a processing error.
The new client asks for company to return the extra £60,000 to a specific bank account. The company returns the £60,000 using online banking and dispatches the goods for the original £2,000 order.
A few days later the company realise that the £62,000 payment was actually a fraudulent cheque paid in at a branch counter and has been returned unpaid. They’ve lost £60,000 in cash and £2,000 in goods.

For any new or unknown customers with no transaction history, insist on the cleared payment being received before any overpayment of funds are returned.

## Malware

This is malicious software such as computer viruses and Trojan horses. Malware is often hidden in attachments and free downloads. It can interrupt your online banking sessions and present you with a fake, but seemingly genuine screen prompting you to enter passwords and codes which can be captured. This information can then be used by fraudsters to access your online accounts and make fraudulent payments.

The advice from Lloyds Bank is:

- When using online banking look out for unusual screens or pop-ups, particularly asking you to input passwords or security codes at an unusual stage.
- Alert your staff to the risk or possibility of devices becoming infected by malware. Ensure they think before they click on attachments or links included in an unusual or unexpected email.
- This has also been known to arrive in the form of an email purporting to be from a known supplier attaching details of an invoice or settlement details.
- Set your online banking so that two separate people are required to set up new payment instructions or to make a payment.  If you can have designated PCs which are only used only for online banking and not email or web surfing activity, they are less likely to become infected with malware.
- Never do online banking from free/open Wi-Fi connections.
- If you see any errors about the site not being secure, stop what you are doing.  Do not log on or complete any transactions.

## Ransomware

This is a more sinister type of Cyber Fraud that is on the increase. This is an extortion scheme where all your files are locked down by malware until a ransom is paid (ransomware). Make sure that you have a backup of any critical data on your computer that is not always online (or the ransomware will lock up your backup as well).

## Reputation Attacks

Another extortion scam is where the perpetrators, who call themselves the "Reputation Killer Team" (RepKiller) have been sending emails to businesses across the UK demanding payment in untraceable Bitcoins (digital currency) by a certain date and time. If the demands are not met, the team have threatened to launch a cyber attack against the businesses and their reputation by automating hundreds of negative reviews online.
The emails also claim that once actions have started, they cannot be undone. Although these scammers are currently calling themselves "RepKiller", it is common for fraudsters to continually change names and adopt new tactics – email names can be made and changed easily.

Whether the attack is attempted or successful, you should report it to Action Fraud on 0300 123 2040 or by using their online reporting tool and receive a police crime reference number.

The advice from Get Safe Online is:

- Do not pay the demand. There is no guarantee the scammers won't launch an attack and could encourage further extortion demands in the future.
- Retain all the original emails. Should law enforcement investigate, the information contained within the email headers can be used as evidence.
- Maintain a timeline of the attack recording all times, type and content of contact.

## E-Commerce

E-Commerce is an important and growing part of our business. The biggest issue that Treasury needs to be aware of is the increased risk of credit card fraud via e-commerce sites. You should make sure that your company's site has fraud detection enabled on credit card transactions.

## Internal fraud

Cyber Fraud may also involve internal employees, either by their direct action or by intentionally assisting an external party in return for compensation.
Continue educating your employees in risk management and promote whistleblowing, i.e. when a worker passes on information concerning wrongdoing.

# PREVENTATIVE ACTIONS

## Treasury policy

It is essential to have a clear internal Treasury policy that outlines the roles and responsibilities within the Treasury department and within the wider Group, especially when it involves processing ad-hoc/one-off manual payments. Ideally, all regular third party payments should be 'locked' down in your banking system or the system you use to input your payments (i.e. amendments to those templates cannot be made easily).

## Treasury processes

Treasury processes should be formalised and communicated to all personnel, as needed for their individual responsibilities. Implement processes to follow, but also explain the 'why' as well as the 'what' to ensure a full understanding.
Have a robust Joiners, Movers and Leavers process to manage access to systems to only those who need it, and ensure access is removed when no longer needed.
This could include further segregation of roles to require two or more people to complete a transaction (i.e. dual approvals, call backs, etc.), but keep in mind that this may require additional time and resources where implemented.
Know Your Employees. It is important for line management to be close to their employees and take time to get to know and understand them.
Create a culture that makes it easy to report suspicions of fraud, but that is also careful to protect innocent employees from unfounded accusations. Report and publicise confirmed internal fraud events as a deterrent to others.

## Treasury controls

Ensure that your processes throughout the group are reviewed regularly, preferably by someone with a strong compliance background. All external third-party vendors that we share data with should provide appropriate verification of their security controls. Work with your local IT department to insure that the IT Security team is reviewing the vendor's security.
Implement checks that ensure your controls are being complied with – internal and external, e.g. monthly, half yearly, annual review of user profiles, a review of all bank accounts held by your company/group.

## Password security

Educate your staff on password security and ensure they create strong passwords both on company-owned systems and on third-party systems used for business purposes (i.e. banking and payment sites). You should not use the same password on different external sites.  You should not use your internal password on external sites. They should be familiar with the password policy that is defined in the company's User Acceptable Use Policy. Remember to treat your password(s) like underwear, i.e.

- change them often
- do not leave them where other people can see them, and
- do not lend them to others

## Specialist advice

Keep updated and subscribe, if appropriate, to advice from external consultants, specialist websites, or reputable journals. You can always contact your local IT support team or the Information Security team with questions or to help with problems. If you don't have this type of resource, then refer to the Get Safe Online team.

## Communication

Do not neglect communications and interactions with your banks and third parties, even if it is only once, ideally twice a year. Scams generally rely on the lack of communication between parties or a lack of understanding of how a third party will typically interact with their customer, e.g. banks will never telephone you and request your user ID and password.

## External banks

Check with all your banks that the processes they apply, not just in the UK, but also in other countries meet your company's requirements. For example in France, the state laws generally override any bank mandate or instruction a company may agree with their bank. Therefore, even if the company instructs the bank to request two signatures on all payments, the President of a French company could enter a local bank and instruct them to make the payment on one (his or her) signature. Some French banks are able to provide a solution that mitigates this risk.

## IT systems

Ensure that you plan for the possibility of a Cyber Fraud incident, where company systems may not be available or data has been destroyed (i.e. by Ransomware).
It is important that you understand the Data Backup and Disaster Recovery plans that your IT team has in place for the major IT systems that your Treasury Team use. This plan will detail what systems the IT department is managing, how often they are backing them up and what would happen in the event of a disaster. This also includes how long systems will be offline, what is the potential for loss of data, what the recovery priority is for your IT systems.  You need to understand this and sign off on it.

Additionally you need to have a Business Continuity plan that documents how your department will continue working in the event of a disaster such as the loss of your IT individual systems (PCs, laptops, etc.), or the loss of the building that your team works in.

## Insurance cost

Shareholders expect companies to protect their interests and ensure appropriate steps are taken to safeguard shareholder value; hence most companies will take our some level of insurance against Cyber Fraud.

Identify how big a risk this is for your company and then mitigate higher value risk. Identify the top risks to your company and insure against them.

Some examples of the top risks that are covered by a good insurance policy are:

- Loss, damage or distortion of own data
- Forensic costs
- Technical support to restore systems & data

Be transparent with your insurers and update them on your infrastructure so they can assess what would form the basis for a 'big' claim.

Make sure the process between your insurer and their underwriter is fully understood and covered.
Ensure you cover not only the consequences of a risk event, but also the causes, e.g. theft of data or payment fraud. Educate your colleagues on what's covered in the insurance policy. This is not just to protect financial risk but also to protect against reputational risk. This is best practice for most companies today.
It is wise to have a crisis plan in place on how to deal with a potential cyber attack on your systems. This is often a requirement by your insurers.
Ensure you are up to date with the latest regulation and legal Acts, e.g. the new UK Insurance Act scheduled for August 2016 is widely expected to re-dress the balance in favour of the insured.

## Crisis response plan

The company should have a crisis response plan to quickly address any major risk or event, including Cyber Fraud. The plan should include scenarios for different types of events and define who is responsible for each step of the plan.
History has shown that an effective crisis response plan can make the difference between a company suffering significant losses in a crisis and one that recovers quickly and maintains customer trust (see graph under Reputational losses).
The Treasury team should have representation on a crisis team, including a primary and alternate person, and be engaged in discussions.

# RESPONSE TO CYBER FRAUD

In the event of a confirmed Cyber Fraud event, always notify the Company Crisis Team immediately.

- Cyber Fraud usually relies on the transaction being processed urgently, so companies need to recognise that fraud is being perpetrated and intervene quickly.
- If you experience any of the listed scams or receive something that seems ‘off’ or not quite right, contact your local IT support team immediately and tell them you have a security concern. They will direct you to someone that can check your concern and help determine if the situation is legitimate or is a larger problem.
- Some carefully planned attacks may take place over a period of weeks or even months. For this reason, be alert if you discover a series of suspicious requests, activities or anomalies (i.e. out-of-balance accounts).
- Let the Crisis Team handle all communications to the public, customers, employees, and business partners. It’s essential that the right messages are communicated correctly to avoid unnecessary financial losses or damage to the company’s reputation.

# CONCLUSION

The purpose for this article was not for it to act as a definitive guide on Cyber Fraud as (a) I am not an IT expert and (b) there are experts that are much better qualified than I am on the subject. I was, however, keen to highlight the areas in Treasury that I am aware have been the target of various scams. Furthermore, I believe it is important to discuss this issue and increase awareness of it amongst our treasury colleagues and peers.

At the very least, my hope is that treasurers read this article and, if they have not already done so, conduct a full review of their key treasury processes including payments.

It is interesting that technology is the main vehicle for Cyber Fraud! Technology also plays a key role in combating Cyber Fraud. The weakest link and strongest asset is you!

Contributors:
Lloyds Bank
Get Safe Online
Action Fraud
Wolseley IT

Royston Da Costa has over 25 years experience working in Treasury. He joined Wolseley in April 2002 as Group Assistant Treasurer and was responsible for managing the daily debt and cash requirements of a large international group.

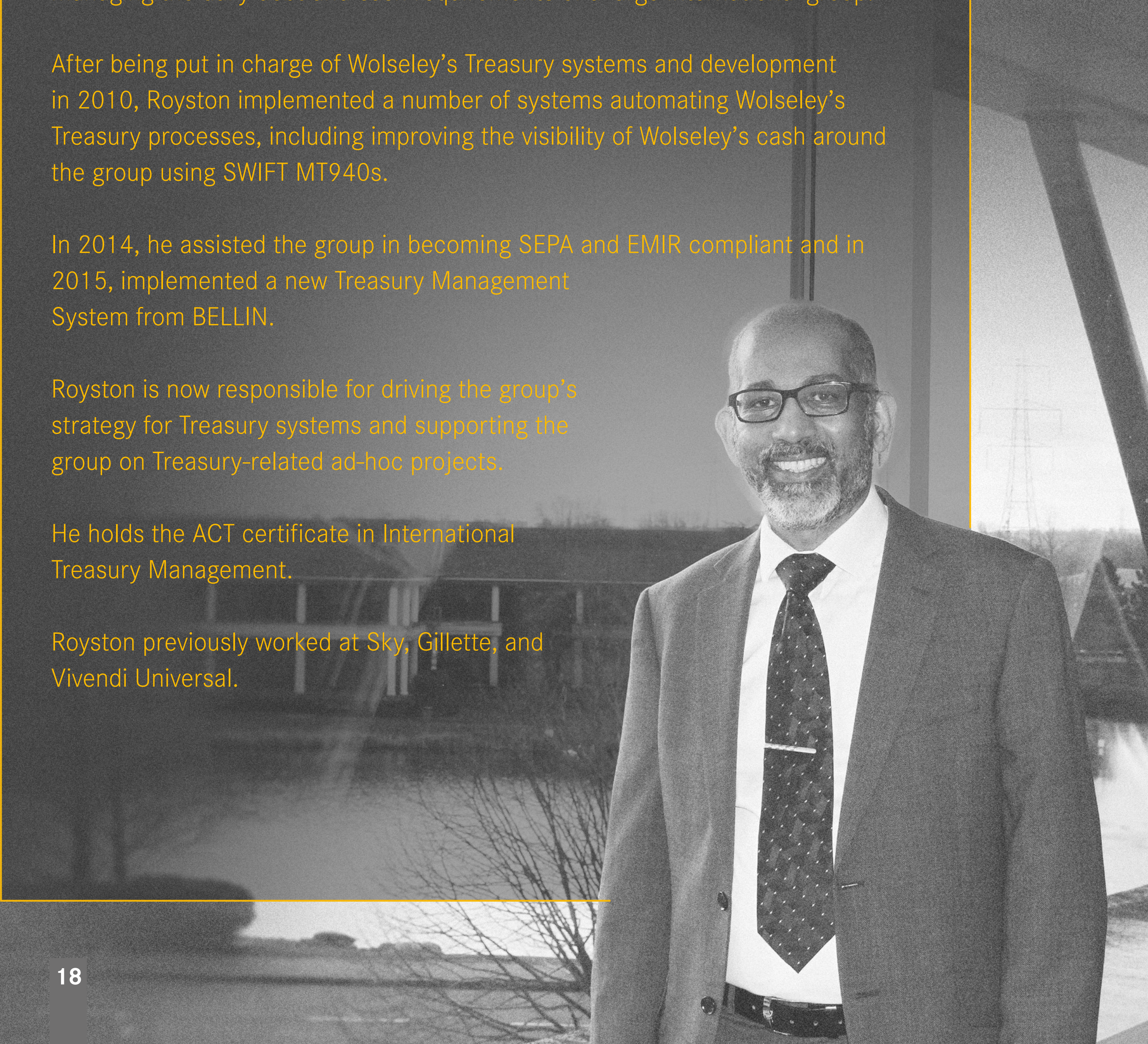
After being put in charge of Wolseley's Treasury systems and development in 2010, Royston implemented a number of systems automating Wolseley's Treasury processes, including improving the visibility of Wolseley's cash around the group using SWIFT MT940s.

In 2014, he assisted the group in becoming SEPA and EMIR compliant and in 2015, implemented a new Treasury Management System from BELLIN.

Royston is now responsible for driving the group's strategy for Treasury systems and supporting the group on Treasury-related ad-hoc projects.

He holds the ACT certificate in International Treasury Management.

Royston previously worked at Sky, Gillette, and Vivendi Universal.



BELLIN. Treasury that Moves You.

bellin.com

**BELLIN GmbH**

Tullastraße 19
77955 Ettenheim, Germany
+49 7822 4460-0

**BELLIN Treasury Services Ltd.**

Suite 1022 - 470 Granville Street
Vancouver, BC V6C 1V5, Canada
+1 604 677 2593

**BELLIN Treasury Alliance Ltd.**

111 Buckingham Palace Rd.
London, SW10SR, United Kingdom
+44 20 7340 8650

welcome@**bellin.com**