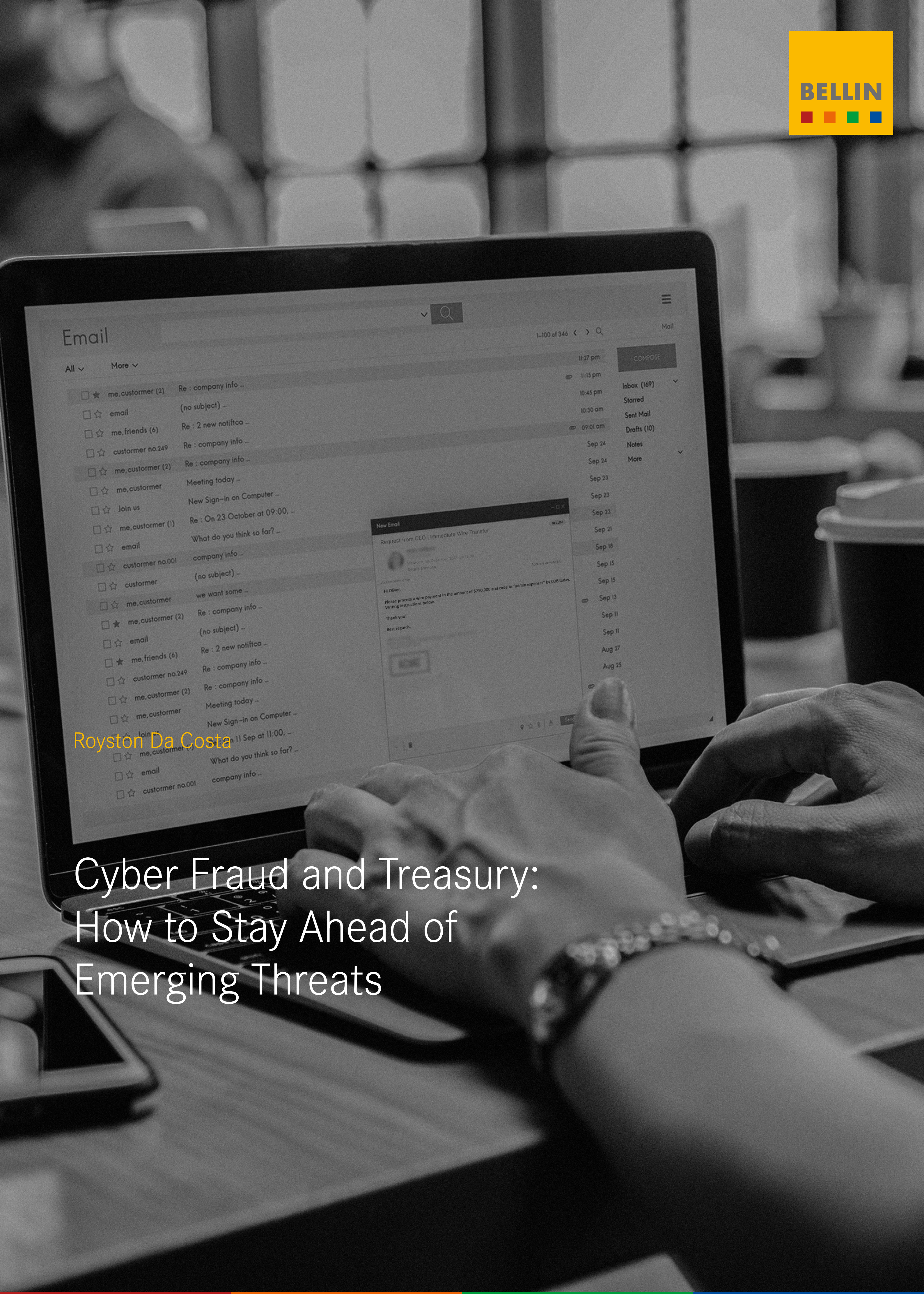
BELLIN


Email
All
More
COMPOSE
Inbox (169)
Starred
Sent Mail
Drafts (10)
Notes
More
me, custormer (2) Re : company info
email (no subject)
me, friends (6) Re : 2 new notifica
custormer no.249 Re : company info
New Email
Request from CEO | Immediate Wire Transfer
Hi Oliver,
Please process a wire payment in the amount of $250,000 and code to "admin expenses" by COB today.
Writing instructions below.
Thank you!
Best regards,

Royston Da Costa

Cyber Fraud and Treasury: How to Stay Ahead of Emerging Threats

Index

Introduction

Cyber criminals always attack the weakest link. Every corporation's greatest asset – and biggest weakness – is the men and women who stand on the front line against cyber attacks. Having clear procedures and practices in place to counter the many threats that new technology brings has become an essential part of good treasury management.

An increasing awareness of Internet fraud is making treasury departments deploy smart and innovative practices in their operations and risk management policies. Many are undertaking a thorough review of internal and external processes. Every component of treasury management – from the supervision of payments to data security – must be robust, fulfilling best practices while also being fully regulatory compliant.

The important role played by treasury in the realm of cyber security was underlined by the J.P. Morgan AFP Payments Fraud and Control Survey, which found that 67 percent of payments fraud was discovered by an organization's treasury staff. To successfully combat cyber fraud, it is vital for treasury departments to have clear channels of communications. Worryingly, many corporations are still failing to ensure effective levels of communication have been put in place between different departments and silos. Some businesses are forced to pay a huge price for such negligence. Criminals motivated by huge ill-gotten rewards are concocting ever more ingenious ways of using technology to commit cyber fraud. Trustwave, a specialist information security company, conducted a study that found cyber criminals expect to make a staggering average return on investment of 1,425 percent. It is of little surprise that cyber crime is evolving in sophistication with new scams continually being propagated against corporations.

In the following sections we will dive into the consequences of cyber fraud, provide examples of attacks and ultimately address preventative measures and responses that every treasury department can implement:

- **Cyber fraud consequences**
- **Cyber fraud examples**
- **Preventative actions**
- **Effective cyber fraud response**

Cyber fraud consequences

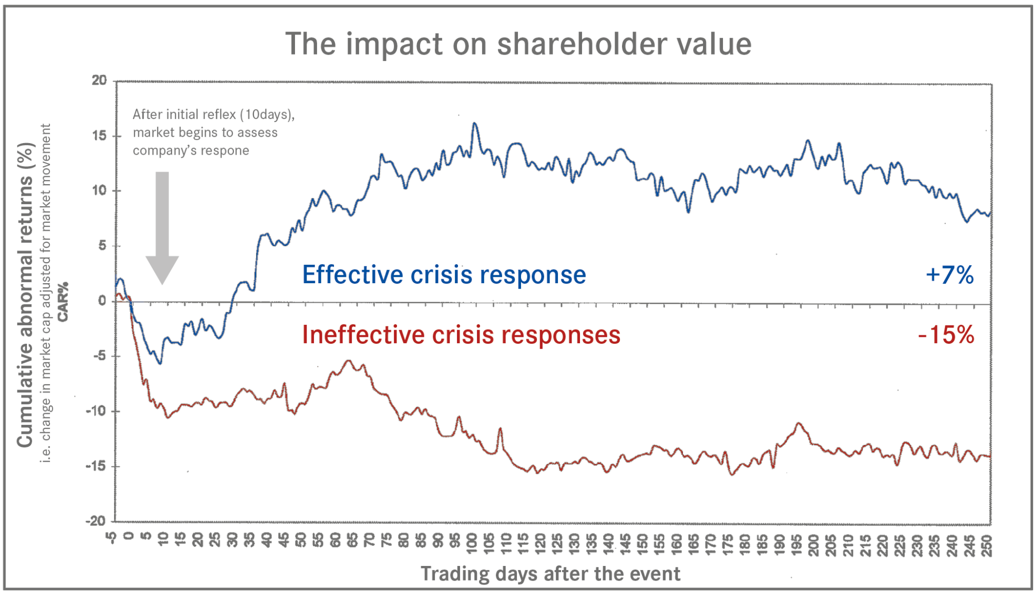
Financial losses

The impact and size of losses that arise because of a cyber fraud event are determined by a variety of factors. These include the time it takes for a corporation to detect that an incident of fraud has taken place and the measures put in place to minimize the size of the loss. In addition, a corporation may suffer further losses if business operations are obstructed as a team investigates the incident and resolves any outstanding security issues.

Cyber fraud can further disrupt the operations of a business if new measures and procedures need to be put in place to close any weak points that may have contributed to the incident. Additional staff training and the implementation of new systems and procedures may also be required.

Reputational loss

A corporation's reputation is at risk in the wake of a cyber fraud attack. Reputational damage because of an incident of fraud can result in a loss of customers and a decline in sales. It is vital for a treasury department to have the capacity to respond quickly after fraud has been detected. Putting in place good channels of communication across an organization enables a speedy response and recovery.



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

Indeed, a corporation's capacity to quickly detect fraud and put in place effective recovery procedures is a good indication of how robust processes and financial controls are across the organization. A failure to respond effectively can have a devastating impact on the reputation of a company listed on a stock exchange, where the sentiment of investors and shareholders carries great weight.

Poor staff morale

Cyber fraud can have significant repercussions on staff morale. Members of a treasury team that have been hoodwinked by a criminal gang can feel a sense of embarrassment or shame, regardless of whether those involved were really at fault or not. The human dimension of cyber crime should never be underestimated. When staff morale takes a hit, it can have long-term consequences on a treasury department.

A fraud investigation to identify a culprit should never turn into a “witch hunt”. No single employee within a treasury department should be responsible for authorizing a payment. While the benefit of hindsight may make scam appear obvious, even the most diligent employee can unwittingly become a victim of fraud. Robust controls within a treasury department should ensure that transactions are thoroughly vetted before payments are approved.

A major incident of fraud can leave a project team or entire treasury department left to take the blame for the breakdown in controls that led to the incident. The subsequent damage to the reputation of those involved can leave staff feeling isolated. In some circumstances, staff may lose compensation or fall into ill health. The person responsible for authorizing a fraudulent transaction may have been a diligent and honest member of a corporation who made an error because he or she did not have any support from colleagues when the incident took place. Rather than an individual being blamed for an incident of fraud, it is the business processes within a corporation that should share the blame. A rare exception to this rule is when a rogue employee circumvents controls within an organization to commit fraud.

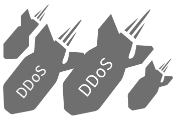
The most common types of cyber fraud

The following examples highlight some of the most prevalent types of cyber fraud:

E-commerce

E-commerce plays an increasingly-important role in the operations of a treasury department. A major risk stemming from the growth of e-commerce-related business is credit and debit card fraud. E-commerce brands typically deal with high volumes of transactions on a daily basis. This opens the door for fraudulent purchases, refund scams, and many more digital payment related scams.

It is vital for a corporation to ensure its website has the appropriate fraud detection systems in place to guard against card fraud. Implementing appropriate return policies can also mitigate micro scams with fraudulent refunds.



Distributed Denial of Service (DDoS)

Increasingly powerful Distributed Denial of Service (DDoS) attacks represent a threat that no treasury department can ignore. In this type of attack, a fraudster will launch a coordinated attempt to overwhelm an online service and knock it offline with an avalanche of Internet traffic sent from multiple sources. DDoS attacks have hit Internet banks and online news services, severely curtailing the operations of these businesses. Digital Attack Map (www.digitalattackmap.com) provides a live data visualization of DDoS attacks across the globe.

The motives for these attacks are often unclear. There is an increasing incidence of so-called hacktivism, where hackers launch a high-profile attack on a well-known website as a means of hijacking a public forum to promote their views. Attacks have even been reported on online retail websites, along with government agencies. The sheer scale of some DDoS attacks makes it advisable for corporations to obtain specialist support to have the appropriate levels of security against this emerging threat.

Fake news

In a digital age, disinformation and fake news can travel fast. When damaging and false information goes viral the impact on a corporation – and its share price – can be huge. For example, Vinci fell victim to a hoax in November 2016 when it was falsely alleged that the French construction and infrastructure company had been hiding losses of €3.5 billion. While Vinci acted quickly to refute the false allegations it was not able to prevent its share price plunging as much as 18 percent.

Major corporations can rely on media relations staff to monitor news alerts, enabling a rapid response to any incidents that may harm the reputation of the company. Businesses that are not large enough to have an in-house media relations team can enlist the services of external PR agencies. Staff should also be encouraged to monitor media noise relating to their company that may have the hallmarks of so-called fake news. The following guide can be used to spot signs of a potential fake news incident:

- Has the story been reported anywhere else? This is a good starting point to quickly establish if a news item is genuine.
- Is the news being reported in broadcast or print media?
- Is the organization reporting the story a well-established news source?
- Does the website reporting on the event appear to be an established news source?
- Does the website address at the top of the page appear genuine?
- Does an accompanying photo or video with a news item look genuine?
- Does the news item sound believable?

Internal fraud

Beware of the enemy within. Cyber fraud threats can emanate from inside an organization. Whether committed by someone acting alone or by a rogue employee assisting an external attack the results of internal fraud can be devastating. It is essential to keep employees informed with the latest risk management procedures. A culture of whistleblowing, whereby workers pass on information of wrongdoing, is also an important defense against internal fraud.

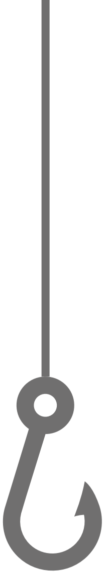
Christopher Grupe launched an attack against his employer, Canadian Pacific Railway, that court documents estimate cost the business $30,000 in “lost business.” Grupe’s attack consisted of deleting configuration files, removing administrative level accounts and changing passwords on the switches of the core network. If an accident had occurred because of his unauthorized access, his employer could have suffered millions of dollars in losses because of damages or fines.

Malware

Malware is often hidden in attachments and free downloads. The malicious software usually takes the form of a computer virus or Trojan horse. In some cases, a malware attack can interrupt an online banking session, presenting a victim with a fake screen that appears to be genuine, prompting him or her to disclose passwords and security codes. This type of attack is used by fraudsters to obtain access to online banking facilities to make fraudulent payments and can even circumvent two-factor authentication.

A bank offers the following advice:

- When banking online, look out for unusual screens or pop-up windows, particularly those that request passwords or security codes.
- Make sure staff know the risks of devices becoming infected by malware. Staff training should make employees always think before clicking on attachments or links, especially those in an unusual or unexpected e-mail. In some cases, a fraudulent e-mail purporting to be from a known supplier will request payment of an invoice.
- Set up online banking so that two separate people are required to set up new payment instructions or to make a payment. Companies that have designated PCs, which are used only for online banking and not e-mail or web surfing activity, will be less at risk of becoming infected with malware.
- Staff should never do online banking from free or open Wi-Fi connections.
- Employees should be vigilant and terminate an online transaction where textual errors indicate that a website may not be secure. Employees should not log on to suspicious websites or complete a transaction in circumstances where personal data may be compromised.



Phishing

Phishing is the most prevalent type of cyber fraud. Criminal gangs send fake e-mails that purport to be from an intended victim's bank or a trusted organization with the aim of eliciting personal data such as bank account details or passwords. A phishing e-mail will often contain a link to a fake website that appears almost identical to the legitimate address. Alternatively, a link may be enclosed in an attachment. The message will usually urge the recipient to act or otherwise risk losing access to online banking facilities.

Experts recommend:

- Bank customers should never click on to links from e-mails that purport to be from their bank. There are a variety of steps that can be taken to first ascertain if the link is authentic or not. The genuine web address can usually be viewed by hovering over the website address link. Alternatively, a long click can be made via a mobile device, whereby a user performs a search, clicks through on a result and remains on that website for a long period of time. If an e-mail requests action, the recipient should either go to the website via a saved favorites link or manually enter the address into a web browser.

A bank offers the following advice:

- Be highly suspicious of e-mails that are poorly-worded or contain spelling mistakes. An authentic bank e-mail will address a customer by their name and contain unique reference points.
- A bank will never ask customers for their password details, card and reader codes, or direct him or her to a screen where this information is requested.
- When in doubt, call a trusted contact telephone number to verify the authenticity of the e-mail.

Ransomware

In a Ransomware attack, cyber criminals use malware to lock down files holding business critical information with the aim of extorting a ransom. Even if a ransom is paid there are no guarantees that the stolen data will be returned. A fifth of corporations that pay a ransom are unable to obtain access to the stolen information.

Ransomware is not a new type of crime. Reported incidents of this form of malware attack date back to the eighties. Still, this type of crime is on the rise with attacks having doubled since last year, according to Verizon's 2018 Data Breach Investigations Report. Ransomware was evident in 39 percent of malware-related cases in this year's Verizon report, with attacks now impacting business critical systems rather than desktops. While this is leading to bigger ransom demands, a corporation suffering a ransomware attack may discover that a criminal's real intention is to disrupt its operations rather than extort money.

Cyber criminals' ingenuity for launching ransomware attacks has led to a series of major incidents making headline news across the globe. One named Petya targeted the Ukrainian central bank and caused major disruptions at Kiev airport and across the city's metro network before rapidly spreading to at least 60 other countries. Meanwhile, the so-called NotPetya, BadRabbit and WannaCry attacks have caused chaos across the globe.

In December 2016, international law enforcement agencies launched a co-ordinated measures against mushrooming incidents of ransomware and banking Trojans, dubbed Operation Avalanche. The operation uncovered alarming evidence of the size and scope of this pernicious strain of cyber crime: Hundreds of thousands of Internet domains and 39 servers were used by the Avalanche network. Meanwhile, 40 different countries were involved in hosting some of the world's most pernicious malware as well as several money laundering operations. Furthermore, as evidence of the growing threat, according to the 2018 Treasury Fraud & Controls Survey Report, three times as many global corporations have experienced a ransomware attack in the period between 2017 and 2018 compared to the previous year. The report also found that nearly one in four firms have experienced a ransomware attack.

The best defense against a ransomware attack is to ensure up-to-date business critical data is securely backed up. In addition, a company should make sure that there is a backup to a USB drive. Corporations that store data in the cloud should check that previous versions of files are also available. Otherwise, a treasurer may find that the restored files are encrypted.

Reputation attacks

As the name suggests, a RepKiller attack aims to destroy the reputation of a corporation. Criminal gangs seek to extort money from a business by threatening to launch hundreds of negative online reviews. Given the importance of a Google search as a valuable source of information on a company, the impact of such an attack can be devastating. The intended victim will often be given a deadline to make a payment in Bitcoin to an account that is extremely difficult to trace.

E-mails sent by the criminals claim that an attack can't be halted after it has been launched. While the perpetrators of these types of attacks currently call themselves "RepKillers", fraudsters frequently adopt different aliases and tactics. E-mail accounts set up by such criminals are almost impossible to trace. Any type of RepKiller attack – whether successful or not – should be reported to the relevant authorities, locally.

Get Safe online (www.getsafeonline.org), a UK-based service offering consumers advice against cyber fraud, provides clear instructions:

- Never pay the demand for cash. There is no guarantee that the criminal gangs won't launch an attack that could encourage further extortion demands in the future.
- Retain all the original e-mails. Should law enforcement agencies investigate, the information contained within the e-mail headers can be used as evidence.
- Maintain a timeline of the attack, detailing a record of the time, method and content of the attack.

Smishing (SMS/text messaging)

So-called smishing attacks – whereby criminal gangs send victims deceptive SMS text messages – are on the rise. Regardless of whether an unsolicited message comes in the form of an SMS text or e-mail, the same precautionary measures must be taken. The authenticity of an SMS text message should always be verified.

A typical smishing attack can appear to be a company informing you to change your password or confirm your account on a service you never even signed up for. The text will include a link or downloadable attachment that is intended to obtain your login information, download malware, or a host of other possibilities. Be very wary when downloading attachments or providing user information to unknown senders.

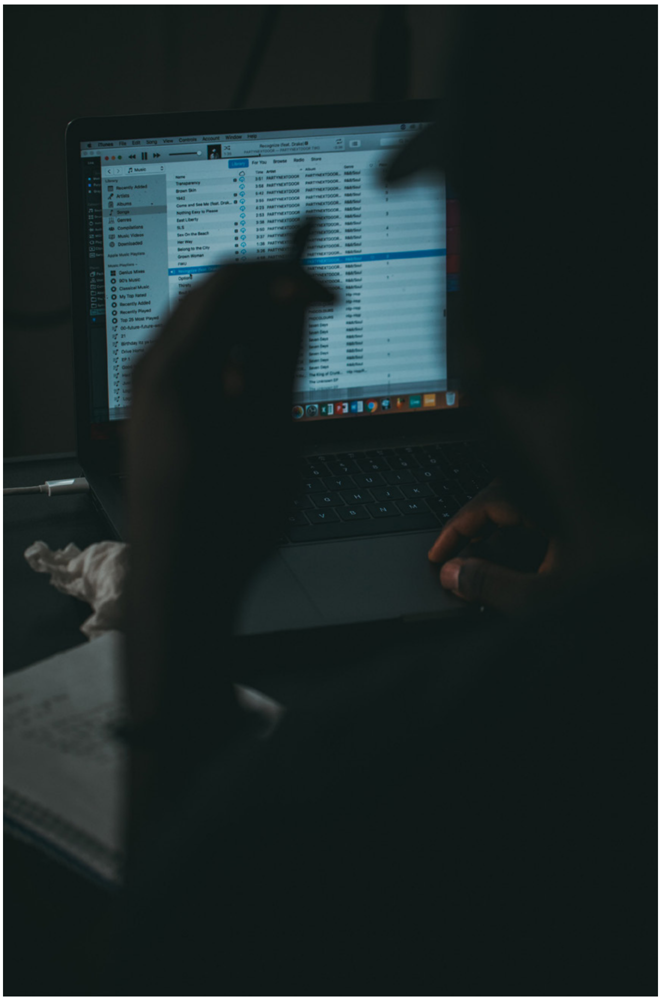
A good rule of thumb is to block the sender and delete the message if it looks suspicious.

Spoofing

So-called spoofing attacks can be done over the telephone or via e-mail. Criminals can use technology to alter the incoming number on a phone's caller display screen to one that appears to be from a genuine bank. Alternatively, a fake e-mail is sent that purports to be from a senior bank employee, requesting that an urgent online payment be made. Whether the ruse is made via e-mail or telephone, any business that does not have systems in place that prevent a single employee from authorizing a payment is at risk of being targeted by this type of scam.

Fostering a corporate culture that encourages employees to ask questions about any payment that looks suspicious is the first line of defense against spoofing. Staff should feel comfortable first consulting with colleagues before authorizing a payment. A good treasury department should foster a culture of questioning transactions that at first glance may appear routine. Some fraud attempts are successful because the staff authorizing the payments assume that the instructions came from people higher up in the corporate hierarchy.

Recently, there has been a wave of spoofing attacks in France. Carole Gratzmuller, the president of Etna Industrie, a medium-sized industrial equipment company based in Paris, was the victim of a specialized e-mail phishing attack dubbed "fraude au president" in France. "My accountant was called on Friday morning," she told BBC News. "Someone said: 'You're going to get an e-mail from the president, and she's going to give you instructions to conduct a very confidential transaction and you're going to have to respond to whatever instructions she gives you'." The accountant was then e-mailed from an address with Ms Gratzmuller's name in it, explaining that Etna Industrie was buying a company in Cyprus. The e-mail said the accountant was going to get a phone call from a consultant working with a lawyer, who would then give her instructions as to where to transfer the money. A stream of spoof e-mails and phone calls followed, pressuring the accountant into sending the money payments. Before noon the accountant had authorized wire transfers, totalling €500,000 to foreign bank accounts. Fortunately for Etna Industrie, banks held up three of the wire transfers, while the company was able to reclaim the €100,000 that went through, according to the BBC News report. "It's like when your house or apartment gets broken into," said Ms Gratzmuller. "You feel vulnerable. People get into your life and they know things about you and you have no clue, and they take things from you."



French businesses have lost an estimated €465 million since 2010, according to a BBC News report that quoted official government figures, with 15,000 firms falling victim to the scam, including major corporations such as Michelin, KPMG and Nestlé. Spoofing attacks are also on the rise in the UK. Belfast City Council lost more than £300,000 when conmen pursued outstanding invoices obtained from a legitimate contractor and hoodwinked staff into sending payments to a bank account under their control.

Meanwhile in the US, the FBI's Internet crime center or IC3 estimates that about 7,000 companies have been defrauded of more than $740 million between 2014 and 2016 in so-called business e-mail compromise scams. Still, companies' reluctance to publicize such incidents due to the subsequent reputational damage makes it very likely that the real figure is much higher.

A bank offers the following advice to guard against spoofing attacks:

- Ensure all employees involved in the processing of one-off payments and regular invoices are made aware of potential scams.
- Have a documented process that ensures all new payments or amendments made to existing payment details are independently verified to ensure that the request is genuine.
- Any concerns that a requested payment is not genuine should be acted upon immediately. Staff should contact the person who made the request via a new e-mail (not a reply) or call the sender directly (using a number from an internal phone directory) to verify the request.

The fraudulent invoice scam part I

In this scam, an employee is unwittingly duped into changing the payment information of a trusted supplier. A typical example of this type of scam takes place as follows: The company regularly purchases services from a supplier, ABC Consulting. A fraudster sends a letter to the company on what appears to be official ABC Consulting headed letter paper. The letter states that ABC Consulting has changed its bank details, quoting a new sort code and bank account number to which all future payments should be made. A company falling foul of the ruse will unwittingly amend the ABC Consulting bank account details in their payment records held with their bank or internal Accounts Payable (AP) system. When ABC Consulting sends the next monthly invoice of £60,000 for services supplied, the company instructs its bank to send the payment. The £60,000 is sent to the new bank account details provided by the fraudster. ABC Consulting later contacts the company for chasing the non-payment of the invoice, resulting in the fraud being discovered. By this time the defrauded funds are extremely difficult to trace.

To guard against this type of scam, a company should:

- Obtain independent verification of any change in the bank account details of a trusted supplier.
- Preferably, obtain approval from an employee working in a different department.
- Avoid using contact details on a suspicious invoice as a fabricated invoice could also be part of the scam.
- Perform an Internet search or use resources offered by a government agency that houses data on registered businesses for identity confirmation.
- Use a highly-secure supplier verification tool like the BELLIN GTB Hub app.

The fraudulent invoice scam part II

In this variation of the fraudulent invoice scam, a company employee is targeted with a request to send a payment to an unauthorized recipient. Such a ruse can unfold as follows: An employee receives an e-mail that appears to be from a senior colleague, such as the Chief Financial Officer. An overdue invoice is attached with the e-mail that makes an immediate request for payment. The targeted employee in such a scam is asked to make a wire payment to the bank account details displayed on the invoice.

All company employees must be made aware that in such circumstances an attachment should never be opened. The senior management of a company would never make such a payment request without an existing invoice already registered within internal systems. Such attachments are either fake – including fraudulent bank account details – or contain a computer virus that can infect a victim’s computer and allow the criminal to steal online bank passwords.

The check overpayment scam

While my focus is on cyber crime, treasury departments must also have controls in place to guard against offline fraud. Check fraud is still a threat. In this ruse, fraudsters make an overpayment using a fraudulent check and attempt to dupe a hapless employee into making a refund payment to a bank account controlled by the gang. The J.P. Morgan AFP Payments Fraud and Control Survey found that while incidences of check fraud were on the decline, 74 percent of organizations still experienced this type of crime. In a separate survey, the 2018 Treasury Fraud & Controls Survey Report found that 18 percent of companies that experienced an incident of check forgery actually suffered a loss.

In the following example I explain how check fraud is perpetrated:

A business receives an order for £2,000 worth of goods from a new client. The client promises to send an online payment to enable the goods to be dispatched. When the company checks its bank account it finds a payment for £62,000. The business contacts the client and is informed that the overpayment is a processing error. The new client asks for the company to return the extra £60,000 to a 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 discovers that the £62,000 payment was actually a fraudulent check paid in at a branch counter and has been returned as unpaid. The company has lost £60,000 in cash and £2,000 in goods because of the payment sting. A business can protect itself from this type of check overpayment fraud by always insisting that a payment must be cleared before an overpayment is returned to an unknown customer.

Vishing (voice phishing)

In this telephone variation of an online phishing attack, a criminal will cold call victims and attempt to hoodwink Internet bank passwords and confidential data or elicit a money payment. For example, a fraudster will call a victim claiming that there is a problem with their bank account and ask him or her to verify their identity by revealing the answers to their security questions. In some cases, a fraudster may also ask a victim to call back on an official number. By holding the phone line open until he or she has called back (a victim never hears a dial tone), he or she can have a false sense of speaking with a bank customer service agent. A request will then be made by the criminal for funds to be transferred to a “safe” bank account under their control.

The advice offered at the Get Safe Online website (https://www.getsafeonline.org/) is that a recipient should contact their bank on a different telephone number to verify the authenticity of the received instructions.

Further advice provided by a bank includes the following checklist to those who fear that an apparent call from a bank is in fact the work of a scam artist:

- Always call back and use a telephone number that is valid, such as one that appears on a bank statement.
- Make sure that a phone line is clear before calling back. Wait five minutes or use a different telephone line if one is available. Never rely on a telephone’s incoming caller display to identify a caller. Fraudsters now have the capacity to make a victim’s phone display a genuine bank number.
- Never divulge a full online bank password or card and reader codes to anyone during a telephone call and never transfer money out of an account unless the intention is to make a payment to someone else.

How to prevent cyber fraud

Implement a comprehensive treasury policy

Clear rules guiding best practice and procedures within a treasury department are vital. The roles and responsibilities of individual employees – particularly relating to payments – should be clearly defined. Regular third-party payments should be locked down, requiring a rigorous vetting process before any changes to payment templates can be made. Stringent guidelines must be put in place for the processing of ad-hoc or one-off manual payments.

Establish transparent treasury processes

Treasury processes and procedures should be communicated to all personnel. Make sure the role and responsibilities of each employee is put on a formal footing. Explain the "why" as well as the "what" when outlining the reasons for best practices and procedures. Clear guidelines should be put in place for joiners, movers and leavers. Use of business-critical systems should be terminated immediately when such access is no longer required. A segregation of duties and roles in the management of payments provides an additional layer of security. No individual employee should be able to authorize a payment or transaction. Payment processes should instead require two or more people to complete a transaction. According to the 2018 Treasury Fraud & Controls Survey Report, 90 percent of global corporations have implemented dual controls for all transactions. Indeed, it is best practice for a treasury department to use a platform that has both payment limits and dual control functions where payment authorizations can be required from multiple people.

Treasury best practice such as reconciling statements in a timely manner can also be highly effective in combatting fraud. A treasury department may also wish to have different people within the department conduct daily spot checks on transactions. "The ability to view cash positions and receive transaction alerts and balances in real time can assist treasury in the fight against fraud, as any anomalous transactions that hit an account can be quickly identified," stated the 2018 Treasury Fraud & Controls Survey Report. "Without daily or real-time visibility, a fraudulent transaction may go unnoticed for several days, at which point it is too late."

A corporation should promote a culture of collaboration and teamwork. It is vital for line managers to get to know their staff and understand their needs. A collective culture where all staff can freely exchange views and opinions can be a powerful defense against the risk of fraud. This can make it easier for staff to report any suspicions that fraud may be taking place. A harmonious work environment can also protect innocent employees from unfounded accusations. Nevertheless, when fraud is uncovered it should be publicized in such a way that it acts as a deterrent to others.

Enact treasury controls

It is vital for a company to ensure a thorough review of processes across the organization on a regular basis. Ideally, a trusted employee with a strong compliance background should be responsible for a stringent review of procedures and practices within an organization. External third-party vendors to whom data is shared should also verify security controls. A vendor's security systems can also be assessed by a company's in-house IT team.

Every corporation should obtain the appropriate compliance certification (minimum SSAE16/SOC1) or equivalent from all third-party vendors and banks. This will confirm that software applications have the required levels of security to repel external attacks. An independent auditor should approve business continuity processes.

In addition, there should be measures put in place to ensure full compliance with internal and external controls. A monthly, biannual and annual review of user profiles is best practice and should be mandatory. A list of all bank accounts held by a company should also be regularly reviewed.

Safeguard passwords with maximum security

Having stringent safeguards to keep passwords secure is essential. Passwords should consist of alpha and numeric characters and be changed frequently. IT security is an important part of staff training, with employees being educated on the importance of password security, both for in-house systems and third-party systems that are used for business purposes, such as banking and payment websites. It is vital that employees use different passwords for internal and external websites. All staff need to be familiar with a company's IT Acceptable Usage Policy. The following steps should be taken by all staff to ensure passwords are kept safe and secure:

- **Regularly change all passwords.**
- **Never write down a password.**
- **Do not lend a password to co-workers.**

Obtain specialist consultation

Large corporations or businesses with a significant online presence should employ specialist staff devoted to cyber security. Some corporations have even made use of ethical hackers to assist them in identifying loopholes in their cyber security systems. While small and medium-sized enterprises (SMEs) may lack the resources to employ specialists in cyber security the threat can't be ignored. In fact, SME's lack of resources in this area has made them a target for cyber fraudsters. Small business owners can keep up to speed with the latest cyber security threats by subscribing to specialist websites and journals and seeking expert advice from external consultants. Businesses without access to IT support or an information security team in their local area should seek guidance from the local regulatory support group.

Clarify communication channels and contacts

Scam artists exploit a lack of communication between different silos within a corporation or a failure among staff to follow the appropriate procedures when communicating with external parties, such as banks or suppliers. Every business should ensure lines of communication are open with key third-party suppliers and banks. A treasury department can seek assistance from a relationship bank in putting proper controls in place. For example, a bank may suggest the appropriate level of controls that are available to a treasury department on its payment platform. Senior staff within a treasury department should also have bank contact telephone numbers to hand, including details of the specialist fraud team.

Businesses should register with their bank for e-mail alerts that provide updates on the latest issues and threats relating to cyber security. Some banks provide customers with a secure hosted portal for the exchange of sensitive information. Webinars are also a powerful tool for obtaining information on issues relating to online security. When registering for this type of service, a subscriber can usually obtain a copy of the presentation and be able to listen to a webinar later if required.

Ensure third-party bank compliance

A corporation should check with all relationship banks that the processes they apply – both domestically and abroad – meet all the necessary requirements. For example, in France, the state law generally overrides any bank mandate or instruction a company may agree with its bank. Therefore, even if a company instructs a bank to request two signatures on all payments, the Chief Executive Officer of a French company could ask a local bank to make the payment on one signature. Still, some French banks can provide a solution that mitigates this risk.

Fortify IT systems for cyber fraud protection

It is vital for a business to have security systems already in place for a cyber fraud attack. A corporation should be prepared for an incident where systems may not be available, or data has been destroyed by hackers, such as is the case in a ransomware attack. The IT department should have a thorough understanding of the data backup and disaster recovery plans put in place for the major IT systems used by a corporation's treasury department. These plans will consider how often IT systems are backed up and what would happen in the event of a disaster event or hacking attack. It is also vital to understand how long systems will be offline, the potential for a loss of data and the recovery priorities of the IT systems. Once an organization has obtained a thorough understanding of all these areas it can sign off a comprehensive business continuity plan governing mission critical IT systems.

In addition, a business continuity plan should also have comprehensive procedures in place for how different departments will continue operations after a disaster. A corporation should be prepared for every eventuality, including the loss of IT systems such as desktop PCs to staff being unable to obtain access to buildings and facilities.

Protect information and data security

It is vital for corporations to ensure that the processing and management of data is compliant with all rules and regulations. The EU has in place stringent regulations to protect personal data. Corporations that fail to ensure adequate controls are put in place risk huge fines. The most serious violations could result in fines of up to €20 million or 4 per cent of turnover (whichever is greater).

The EU's GDPR (Global Data Protection Regulation) requires corporations to protect sensitive data held on proprietary systems, including, for example, drop boxes. The use of drop boxes helps ensure that only approved parties can obtain access to encrypted files.

Designate social networking policies

The increasingly ubiquitous nature of social media – with Facebook, LinkedIn, Twitter, Instagram and WhatsApp – playing a daily part in people's lives has created new opportunities for identity fraudsters. A profile page on a social media platform can provide a treasure trove of information for the criminally minded. Personal data such as a date of birth can be used to impersonate an individual's identity while phishers can obtain the information that is required for launching a sophisticated attack. Everyone should ensure that social media profiles are kept as secure as possible without disclosing key personal data.

Internet of Things

The Internet of things (IoT) refers to the inter-networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable such objects to collect and exchange data. IoT applies to a variety of devices and applications, including smart TVs, wearable smart devices, Wi-Fi printers, thermostats and similar home control devices and even most new cars. Cyber criminals are launching attacks against a variety of IoT devices. For example, attacks are being launched against a victim's network via a smart device. Such an attack could be launched against a victim's home or work network with devastating consequences if the necessary security software has not been put in place.

Insure against fraudulent damages

Most corporations now recognize the importance of specialist insurance policies that guard against a variety of threats, including cyber fraud. According to the 2018 Treasury Fraud & Controls Survey Report, 31 percent of global corporations have a standalone policy for cyber fraud insurance. Stakeholders in listed companies expect high levels of due diligence to safeguard shareholder value. Every corporation should carefully assess the size of the cyber fraud risk that it faces, along with other major risks.

Examples of the primary risks covered by a good insurance policy include:

- **Loss, damage or distortion of in-house data.**
- **Forensic costs.**
- **Technical support to restore systems and data.**

A corporation should always be transparent with an insurance provider and update it on the infrastructure put in place to counter fraud. This helps ensure an accurate assessment can be made in the event of a major claim. A corporation should ensure that the process between its insurer and the underwriter is fully understood and covered. The causes of a risk event – such as theft of data or payment fraud – are as important as the consequences. All employees should be kept informed about what an insurance policy covers. Reputational damage can be as devastating as the more conventional and obvious threats. It is therefore best practice for a corporation to have an accurate understanding of the various risks that it faces and have the appropriate level of cover to guard against these threats. Insurance providers often require a business to have a crisis plan in place to cope with a potential cyber attack. A corporation should also stay abreast of the latest regulations and legislation.

Create a crisis contingency plan

Every treasury department should have a comprehensive crisis response plan in place to ensure a rapid response to a disaster event, such as a cyber fraud attack. A well-prepared crisis response plan should also put measures in place for a variety of different scenarios. The plan should also clearly outline the responsibilities and duties of staff.

History shows that an effective crisis response plan can make the difference between a company suffering huge losses and one that recovers quickly and maintains the trust of its customer base. A treasury team should have representation on a crisis management task force and be thoroughly engaged in all discussions.

How to respond to a cyber fraud

When cyber fraud takes place, a treasury department should immediately contact its relationship bank. If, for example, payment fraud has been identified, a bank may be able to hold the payment until it is validated. A corporation's crisis team should also be immediately notified.

- Avoid rapid-response payments. Cyber fraud typically relies upon transactions being processed urgently. It is therefore vital for staff not to be pressured into making any transactions without following rigorous security procedures.
- Stay alert about suspicious activity. When an employee encounters something that looks suspicious, he or she should immediately contact IT support and relay their concerns. A speedy investigation will uncover any incidence of fraud.
- Keep your eyes peeled for suspicious patterns or activity. Some carefully-planned attacks may take place over a period of weeks or even months. This makes it vital for every employee to be in a perpetual state of alertness and ready to spot a series of suspicious requests, activities or anomalies (e.g. out-of-balance accounts).
- Enlist the support of a specialist crisis support team to handle all communication to the public, customers, employees and business partners. A rapid response approach regarding expert outreach limits financial losses and helps to protect a corporation's reputation.

Conclusion

Cyber fraud represents a rapidly-evolving threat. It is essential for treasury departments to be aware of the new types of fraud that are emerging because of online technologies. The global nature of cyber crime means every business must make sure that security systems are watertight. Gangs can now conspire to defraud corporations from different countries and jurisdictions across the globe.

“In today’s world, more organizations experience fraud than those that do not,” stated the 2018 Treasury Fraud & Controls Survey Report. “Given this reality, there is really no excuse for firms not to have sophisticated control frameworks in place. If your company has not already been targeted for fraud, it will be, and given the current trend, the frequency of attacks will only escalate moving forward.”

I have highlighted the key areas, vulnerabilities and weak points that can emerge within corporations. I believe the best defence against cyber fraud is for a treasury department to have a continual dialog about the emerging threats and discuss the best solutions with colleagues and peers in the industry.

Fact: Cyber fraud is an evolving threat with new technologies being the main vehicle of attack.

Fact: New technologies are playing a key role in combating cyber fraud.

Fact: The weakest link – and strongest asset – is a company’s staff serving in the front line in the fight against cyber fraud.

Royston Da Costa has over 29 years' experience working in treasury. He joined Wolseley, now Ferguson Group, in April 2002, and was responsible for managing the large, international group's daily debt and cash requirements. He was promoted to assistant group treasurer in November 2016, and is now responsible for the middle office. Internally, he acts as the focal point for Ferguson Group's business units on operational treasury issues such as payment connectivity, working capital and transactional banking. Externally, he is the main contact for the group's relationship banks on matters related to payments, regulation and technology. He continues to be responsible for driving forward the group's strategy on treasury technology. Royston previously worked at Sky, Gillette, Seagram's and Vivendi Universal.

Ferguson uses the treasury management system tm5 by BELLIN. They were recognized in the 2018 TMI Awards for Innovation & Excellence with a Corporate Recognition Award for their "Future-Proofing Treasury" project using tm5.

BELLIN. Treasury that Moves You.

bellin.com

BELLIN GmbH (HQ)

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

BELLIN GmbH

Killisfeldstasse 30
76227 Karlsruhe, Germany
+49 7822 4460-0

BELLIN Treasury Alliance Ltd.

Aldwych House, 71-91 Aldwych
London, WC2B 4HN, United Kingdom
+44 20 3865 8401

BELLIN Treasury Services Ltd.

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

BELLIN Treasury Services US Ltd.

625 Massachusetts Avenue
Cambridge, MA 02139, USA
+1 800 251 5385

welcome@**bellin.com**