Transaction Banking
Cybersecurity Whitepaper
Beyond IT Controls
Executive Summary

We are in a digital age, but consideration of the impact of digitalisation is lagging in some areas. This is contributing to a worldwide economic and security problem. What is this threat that is costing the US alone one third of its GDP?¹

Once, cybersecurity may have been the preserve of the IT department. That has long-since ceased to be the case. Nowadays, every single person working within an organisation must understand their role and apprehend their responsibility for their organisation’s cybersecurity defences.

The C-suite in particular must grasp its importance and educate themselves as to the dangers and necessary safeguards. Effective and up-to-date technical controls are essential, but increasingly employees – whether knowingly or unwittingly – are the most frequent cause of security breaches.² They can therefore also be a key defence with the right training and education.

Do you know where the weaknesses lie either within or as part of the walls of your organisation? In an age of invisible threats, both internal and external, how can you defend your organisation and make it impregnable?

²http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
Table of Contents:

I. **Cyberrisk:** The extent of the problem and the reality of the risks
   - Cybersecurity today
   - Corporates and financial services targeted
   - Fraud diversification: The changing nature of attacks
     - Real-world examples
   - Drawing the control lines: Regulatory change

II. **Financial services:** What controls can and do banks implement to defend against cybercrime

III. **Corporates holistic approach to cybersecurity:** What tools are available to corporates to mitigate risks and respond to breaches?
   - Governance structure
   - Culture shift
   - Process improvement
   - Staff training and awareness
   - Technology controls

IV. **The Future of cybersecurity**
   - Tomorrow’s threats
   - Tomorrow’s defences
   - Conclusion
I. Cyberrisk:
The extent of the problem and the reality of the risks

Cybersecurity today
As business has digitalised, it has become vulnerable to a widespread new threat – one that is pervasive but under-addressed. This threat is global, but continues to be underestimated. In fact, it brings staggering losses to organisations year after year, primarily due to internal causes, yet few truly understand it and many feel no responsibility for the consequences.3

From fortresses to vaults, protecting information or value has always been a key concern for governments, communities and businesses. As our world moves online, those security measures need to be stronger than ever – but in new ways and on all fronts – to protect virtual data and assets. But, just like the threats they defend from, such security measures must be far more complex and sophisticated than historic ones, as well as constantly updated.

Unfortunately, not having sufficient measures in place carries a hefty price tag. It is estimated that cybercrime costs the global economy more than $400 billion a year4 and is expected to surge to $2.1 trillion globally by 2019.5 Although cybercrime impacts everyone from governments to citizens, it is businesses that bear the brunt of the damage; a significant proportion of which is caused by the theft of intellectual property and espionage. However, for many corporates the key threat is fraud via cyber-methods, stemming, first, from the crime of identity theft.

Corporates and financial services targeted
Although cybercrime covers a wide remit of offences perpetrated online, from hacktivism to social crimes, for corporates and the financial services it is fraud that is a top concern. Fraud can have knock-on effects such as reduced efficiency and cash flow issues, but who is at risk and why?

Generally speaking, the bigger the organisation, the more attractive the target, but in truth, everyone is at risk. Large banks, the largest MNCs and civil services tend to receive media coverage when they are hacked, but all businesses are at risk irrespective of size or location, with 90% of large companies and 74% of small companies in the UK experiencing at least one security breach last year.6

Unsurprisingly, North America, Europe and Asia are currently losing out the most and Africa the least,7 but as other regions enjoy both greater economic growth and digitisation, attacks will be more evenly-spread globally. Similarly, some industries experience a much higher threat level than others, with healthcare, manufacturing and financial services hit the hardest.8

Nor is the threat purely external – according to IBM research, in 2015 45% of cyberattacks were carried out by malicious insiders (and an astonishing 60% by insiders in general).9 Just as crucial, therefore, are protective measures and deterrents against internal threats – whether

---

9IBM 2016 Cyber Security Intelligence Index
inadvertent or by way of active employee collusion. Employers must ‘Know Their Employees’, as well as recognise that as networks grow and an increasing number of devices become connected, the sources of potential insider threats are also constantly increasing.

Many – if not most – of external cyberfraud attacks now begin with some form of identity theft via email. This means that, unfortunately, even the most well-meaning workforce still poses a significant threat to any company because each of its members is a potential target for cybercriminals. For these, there are basically two ways into a targeted organisation’s data or systems, through software designed to undermine its defences, infiltrate its systems and either steal security details or mimic its employees, or through its people, by means of social engineering – tricking its staff into willingly giving them the access they desire. While many cyberattacks are carried out using malicious software, it is often easier for cybercriminals to trick a person than hack into increasingly well-protected systems. Additionally, in today’s threat landscape very many cyberattacks use both lines of attack, with cybercriminals cleverly exploiting information obtained by using malicious software to bolster the credibility of a social engineering attack, and using information gleaned from unwitting employees to facilitate software attacks.

While “social engineering” may sound modern and technical, it covers some of the oldest confidence tricks in the book, carried out using modern 45% of cyberattacks were carried out by malicious insiders.
channels of communication. Many corporate employees do not realise that – far from being particularly technical – a very high proportion of cyberattacks use normal everyday business communication – an exchange of emails, an SMS or a telephone call – to extract some small piece of personal, company or financial information that will prove vital to the criminal. Equipped with this tiny piece of information, combined with other pieces of information extracted in similar ways or from public information, cybercriminals may go on to steal online corporate identities and credentials, infiltrate company systems, databases and bank accounts and steal millions.

In view of the scale of the threat, it is surprising how many corporate employees are still insufficiently aware of how genuinely ubiquitous “social engineering” cyberattacks are and how subtle and insidious the tricks are that cybercriminals use. Therefore, in addition to implementing and updating technical controls, the most important way in which all organisations can protect themselves against cybercrime is to make their employees understand just how valuable company information – even the most insignificant-seeming snippet – is to cybercriminals, and to educate them in the various ways in which they may be tricked. Put in a different way, every organisation serious about fighting cybercrime must effectively turn its employees into a “human firewall”, by educating them and instilling in them a culture of information security. And whereas cybersecurity may once have been solely an IT issue, nowadays it is also a key C-suite concern; top-down mandates should prioritise not only the implementation and maintenance of proper technical controls, but also employee education and alertness.

**Fraud diversification: the changing nature of attacks**

Information security has come a long way from the earliest ciphers, used for military communications by the ancient Greeks and Romans – and so have attempts to access confidential information, particularly since the first computer worms and viruses in the 1980s. But in the last decade, cybercrime has developed into a fully-fledged, sophisticated service-based industry complete with supply chains, business models and skill specialisation; this is the downside of the rapid technological advancement we have enjoyed.

Cybercrime is likely to continue to rise steeply as the dropping costs of technology continuously lower barriers to entry, the black market for breached data grows, and the IoT and ‘bring-your-own-device’ culture and cloud-based storage become increasingly
prevalent. Security breaches are more frequent, and are costing businesses more, both financially and in the time it takes to recover.¹⁰

One of the main ways in which cybercriminals operate is by manipulating an organisation’s staff; they may trick them into unwittingly downloading malware onto the company’s systems, opening these up to criminal control, or into directly revealing information. Finally, and most brazenly of all, they may persuade them to carry out fraudulent instructions which they believe to have been legitimately given by their corporate superiors. While the forms cyberattacks may take are legion, and inventive schemes proliferate, there are recurrent features and distinct categories.

Cybercriminals are indiscriminate in their use of channels of communication, phishing by e-mail, smishing by SMS messaging, and vishing by voice on the telephone. On the one hand, they cast their net widely, capturing information by using automated email addresses or phone numbers, on the other they target individual senior company officers (CFOs or CIOs), to obtain confidential information or convince them to transfer money out of the company. They piece together fragments of apparently insignificant information, which they build up into a complex picture of how the company works, allowing them to co-opt credentials, abuse user privileges, enter systems or convince employees that their communications and requests are authentic. A name or date of birth here, a password there, a tiny snippet of office procedure – anything may become another piece completing this complex puzzle.

As well as using information gained from other interaction, and channels of communication to make their requests seem plausible, cybercriminals often import a fake sense of urgency into a (fraudulently constructed) situation in order to pressurise their targets to behave as they wish. Time and again, experiments show very high success rates when people are targeted in this way. Social engineering is frequently combined with a software attack, for example with email hacking, which strengthens their combined effect.

For example, criminals may first hack an employee’s email account and then use the information and the credentials obtained to send emails to customers on the company’s customer list requesting payment of invoices into a fraudster-controlled bank account. Or, in an example of (spear) phishing, a payment operations employee may receive an e-mail purporting to be from the target corporate’s banking provider, directing its recipient to a website mimicking that of the bank. Here, s/he is manipulated into sharing ID and authentication details either through a web form or by a ‘customer adviser’. Another route of attack might be an automated recording claiming that a credit card or bank account has been compromised and asking the targeted individual to supply personal

¹⁰http://www.techweekeurope.co.uk/security/cyberwar/uk-business-cybercrime-costs-rise-178506
information via the keypad. The phone number shown on the falsified caller id appears to be that of the target company’s bank. A separate attempt might involve a person pretending to be a bank representative calling to ‘confirm’ details, while actually extracting them, and perhaps following up with an email. Another frequent attack is a fraudster acting as a corporate’s vendor requesting a change to its bank and account number. Then, future payments by the corporate are directed into that fraudulent account.

One form of social engineering that is both widely spread and may be highly damaging is the ‘fake president’ attack. Again, emails are sent – this time internally from a hacked email account, particularly that of a senior or C-suite employee (for example CEO or CFO) – to instruct another employee to make a payment from the targeted company to a fraudulent recipient. For example, a company’s cash manager receives an email purporting to be from his CFO, urgently instructing him to transfer a large sum of money to fund a highly-confidential (possibly hostile) takeover, and telling him he will shortly receive a telephone call from an independent auditor who will provide further details of the transaction. The cash manager receives such a call shortly afterwards from a fake auditor with sufficient company details to make him sound authentic. A remittance form with the CFO’s (fake) signature is then sent via internal post to the cash manager, who confirms the payment with his own signature and puts the form forward to the bank. The bank is suspicious about the unusual transfer and contacts the cash manager via telephone who
confirms the payment is authorised and required urgently. The effort and detail invested in such attacks should not be underestimated – cybercriminals may exchange dozens of emails with potential victims in order to convince them of the sender’s credibility.

**Real-world examples**

A high-value real-world example of this was the loss in January 2016 of around €50 million by Austrian aerospace parts manufacturer FACC, which was reported to have been the victim of a ‘spear whaling’ attack tricking a senior executive of the company to authorise a wire transfer of funds away from the company to an account controlled by fraudsters.\(^\text{11}\) Although spectacular in terms of value, this attack was typical of many modern cyberattacks. Such attacks may be initiated by a technical breach, such as malware spread through a phishing email designed to obtain internal company details, email accounts or telephone numbers. However, the actual execution of the fraud or theft relies on a highly-sophisticated and multi-layered approach targeting individuals and orchestrated across a number of different channels of communication. Most people would not initially connect these approaches to a cyberattack, and, time and again, this throws targets off the perpetrators’ scent. This is where employee education is needed, at all levels of seniority.

Such examples illustrate just how valuable every piece of company information is to cybercriminals, and show the pressing need for organisations to have – in addition to mere technical controls, however important these are – layers of cybersecurity defences relating to governance, culture, people, technology and to processes. Thefts like the ones described above could in many cases be prevented by requiring any payment instruction above a certain value to be confirmed with the authoriser using a separate channel of communication, for example, a telephone call, and by requiring such payments to be independently confirmed by a further authoriser, in appropriate cases even by two further ones.

Perhaps more than any other point, the bank’s telephone call to the cash manager in our example highlights that educating people within an organisation in the principles – and practice – of cybersecurity is of paramount importance in fighting cybercrime. If those with the ultimate authority to release a payment are convinced that a payment instruction is authentic, no technical control – howsoever sophisticated this may soon become e.g. by using biometrics like facial recognition – will prevent fraud or theft from occurring. The only way it might have been avoided is by adding a requirement for authorisation through another channel, or by an additional person – in other words, by steps relating to process, and to people.

When it comes to the more technical forms of cyberattack, there is a bewildering variety of ways in which cybercriminals today perpetrate attacks using malicious software,

\(^{11}\)https://hacked.com/55-million-cyber-heist-strikes-aerospace-parts-manufacturer/
known as malware, to disrupt or gain access to private systems or to gather confidential information. Viruses or worms are self-replicating programmes, the former attach themselves to existing legitimate programmes, the latter use a network to spread to other computers, often via ad-related spam email. These can occur in various forms; botnets (‘zombie armies’), which have been decreed as the biggest threat to the internet today, are networks of malware-infected computers that forward spam, viruses or worms on to other computers; trojan horses embed themselves in a browser application and can then intercept and manipulate any information that the user submits; rootkits hide their own presence yet allow access to restricted areas of a computer or system; key logger robots record keyboard keystrokes to collect user access IDs and account information; and bogus invoice schemes install malware which logs the company’s banking and financial information.

Just how much damage may be caused by a software-led cyberattack is demonstrated by one of the most successful attacks ever, on Bangladesh’s central bank, in February 2016. This aimed to steal $951 million via 35 separate money orders, and in fact managed to extract $101 million before being blocked (just $20 million of which has been recovered at the time of writing, and only due to a spelling error in the name of the recipient account). The perpetrators inserted malware into the bank’s computer systems – which sat undetected for some weeks before the attack – that cloned legitimate transactions before generating the fake wire transfers. It is not yet clear whether the malware was distributed via a social engineering attack such as email spearfishing, which would of course make this an example of both the main ways in which cybercriminals target organisations – people as well as software.

The attack remained under wraps in the immediate aftermath, highlighting the importance of employee responsibility and alertness in such cases, and has also led to calls for regulatory reforms in the region, which is particularly prone to such attacks. While Deutsche Bank flagged up a typo, and the New York Fed blocked 30 transactions, SWIFT and the Fed both claim that their systems were not compromised and that the payments were fully authenticated. In addition to the value lost and the reputational damage incurred by this attack, its partial success may encourage copycat attacks around the world – in particular as high-value SWIFT payments are more worthwhile targets than smaller transactions.

SWIFT itself has called this incident a “watershed” and warned of the threat posed by cybercrime to the global financial community. Besides calling on its members to drastically improve information sharing on cyberattacks, it announced it would support its members in their use of payment pattern controls to identify suspicious
behaviour, and develop security audit frameworks to ensure they tighten up their systems sufficiently.

While losses in the Bangladesh case were high, this is not the largest ever real-life cyberheist. That dubious accolade goes to the Carbanak case, an example of an even more sophisticated software-led attack – an advanced persistent threat (APT) attack – which used complex malware to steal vast amounts of cash over an extended time period. A cybercriminal gang comprising members from Russia, Ukraine, other parts of Europe and China targeted a number of banks’ internal systems and operations, resulting in the theft of about one billion dollars worldwide over a two-year period. The gang managed to go unnoticed for well over a year while continually attacking banks from within. This attack was multichannel, using a combination of technical weapons to take over the target banks’ systems at key points including in their core systems and at user endpoints. Money was stolen from online banking systems, e-payment systems and ATMs. Averaging USD8 million per bank, each bank robbery took between two and four months from infecting the first computer at the bank’s corporate network to cashing the money out.

Both banks and corporates can guard against these and similar attacks by implementing a robust and holistic cybersecurity program covering governance, culture shift, employee training, technology and process review.
Drawing the control lines: Regulatory change

In addition to the continuously morphing nature of cyberthreats, and as governments realise the extent of their cost, laws are being introduced to regulate cybersecurity. In December of last year, the US ‘Cybersecurity Act of 2015’ was signed into law, and other bills expanding on current regulation have been proposed. In the same month, EU lawmakers agreed on new cybersecurity rules in the Network and Information Security (NIS) Directive, to be adopted in coming months, and the General Data Protection Regulation (GDPR) to replace the 1995 Directive 95/46/EC.

Perhaps even more influential is the Payment Services Directive II, also published recently. The PSD2, which repealed the initial 2007 directive, entered into force at the beginning of the year and will be national law in all EU member states by 2018. The new directive has a wider scope with regards to payment services providers affected, but it also – in line with the NIS directive – requires additional client security controls. The PSD2 insists on strong customer authentication, including two-factor authentication for client online banking log-ins, as well as stricter security for remote transactions including a dynamic link to the transaction value and the payee’s account. These requirements from PSD2 are in keeping with cybersecurity laws elsewhere, including the Monetary Authority of Singapore, Hong Kong Monetary Authority and other APAC regulators.

In line with increasing and changing cyberthreats, further regulatory measures will likely unfold in various regions over the coming years, potentially bringing more scrutiny, audits and fines; corporates can be one step ahead by understanding the threats and controls entailed.
While losses from technical, software-led type of cyberattacks can be severe, such attacks are mitigated by putting in place the right kind of – layered, robust and effective – holistic cybersecurity program. Banks, naturally, are already strictly regulated around security. For example, Deutsche Bank has long established a comprehensive information and cybersecurity programme, with a strong security governance framework, to implement controls and comply with security policies and standards. The Bank’s own security policies and standards are codified and updated on a regular basis, and all IT vendors must also comply with them and with Deutsche Bank’s risk assessments and periodic vendor control assessments.

Just as it is for corporates, staff training is crucial for banks. The human element plays a key part in all cybersecurity measures and programmes; so much so that an organisation’s employees should be regarded as – and trained and supported to be – its “human firewall”. It cannot be over-emphasised that when it comes to cybersecurity, employee education and awareness are paramount, and that without them technical controls are almost bound to fail.

Banks of course have a double requirement and incentive to maintain optimal information security because they have to protect both their own data and that of their clients. Deutsche Bank, for example, provides and regularly updates a range of comprehensive information to its employees on information security and current cyberthreats, via its intranet. Web-based information security awareness training is mandatory for all its employees, and videos are frequently posted on its intranet on a range of cybersecurity topics such as phishing, or threats associated with mobile devices. Additionally, Deutsche Bank’s internal simulated phishing campaigns help put employees’ cyberknowledge and skills into practice, as well as bringing home to them the reality of the threat. All these approaches and resources are brought together at Deutsche Bank’s global roadshows on cybersecurity which take employees through a wide range of current threats and teach them how to behave in critical situations, such as how to counter live hacking.

II. Financial services:
What controls can and do banks implement to defend against cybercrime?
Additionally, in a client-facing business such as banking, it is equally important to keep clients aware and informed about potential cyberthreats, and banks are in fact required to do this from on-boarding a client throughout every stage of the client relationship. Best practice includes providing clients with ad hoc alerts and updates on the latest threats detected in clients’ geographical regions and further information and advice to support clients in their own efforts to remain cyber-alert. However, in addition to these people-based measures, in order to mitigate the risk of unauthorised access and manipulations at network-, system-, application- and database-levels, as well as to support data processing standards in line with legal data protection requirements, banks must implement several levels of controls, including physical, administrative and technological controls.

Physical controls restrict access to offices and data centres, ensuring only those who are authorised may enter them. Administrative controls are designed to restrict access to any class of data or system to those required and authorised to access them. These include segregating duties, neutral controls, regular staff recertification, authentication and authorisation, privileged access controls and real time security monitoring. The third and final form of controls are technological controls, including the latest anti-malware and encryption software, network intrusion detection and security patching technology, as well as a dedicated data leakage prevention (DLP) programme, and any proprietary solutions. For example, Deutsche Bank has implemented an industry-leading third-party solution for the detection and deactivation of Distributed Denial of Service (DDoS) attacks.
III. Corporates’ holistic approach to cybersecurity:
What tools are available to corporates to mitigate risks and respond to breaches?

III.i Governance structure
Laying the framework for a cybercrime prevention culture rests with a strong corporate governance structure. Writing, communicating and auditing clear policies – that define risks and provide guidance on acceptable behaviours – is critical to mitigating internal and external fraud.

Creating the most effective organisational structure to manage the cybersecurity program is equally important. Establishing a dedicated cybersecurity team – to establish the cybersecurity framework, prioritise projects and track implementation progression – is the cornerstone of a robust cybercrime prevention program. It is best-practice for this team to report to the Board through the Chief Information Officer or a similar role, in order to elevate the discussion and ensure that the correct messaging is coming from all leadership positions.

Every organisation should have a data protection policy in place that identifies what data is sensitive and vulnerable to attack, and how and where that data is stored. The policy should also lay out roles and responsibilities for data owners and users. Other aspects of this policy can include parameters for penetration testing and intrusion detection. Finally, the policy should explain remediation plans and disaster recovery plans in case an attack is successful.

Other key policies that should be reviewed from a cybercrime prevention perspective include the Payment policy and Counterparty Risk Management policy. The Payment policy should pay particular attention to how wire payments are processed and approved, given the surge in cybercrime in that area. The Counterparty Risk Management policy should require technology partners and suppliers with access to sensitive data (or that help move sensitive data) to have robust cybersecurity programs in place that can be tested and audited, ensuring that ERP providers, treasury workstation partners, payment processors, credit card providers, and so on have the strongest protections in place to prevent cyberattacks.

III.ii Culture shift
Creating a culture where the responsibility for mitigating risks around cybercrime is not borne exclusively by IT, Treasury or Finance, but shared throughout the organisation, is essential. Every employee in an organisation plays a role and shares a responsibility for safeguarding the firm’s assets.

Culture can be sculpted by the norms, behaviours and attitudes of the people within the organisation. But creating this typically begins with behaviours and attitudes from senior leadership. The Board and senior
management must raise cybercrime prevention as a serious corporate-wide priority with clear and consistent messaging. Employees should be encouraged to scrutinise requests that appear out of the norm or look suspicious. Employees should be made to understand the responsibility that they carry and the impact they can make on developing a secure environment. Finally, employees should feel empowered to think and question information, transactions and requests that appear suspicious and should never be penalised for attempting to protect the organisation’s sensitive assets.

All levels of management must participate in clear and consistent messaging about the commitment and seriousness of cybersecurity. Regular updates on the types of scams and fraud are needed to keep the workforce educated. Prevention techniques and changes in policy or procedures should be shared across the organisation with regular emails, newsletters, webinars and/or a dedicated website that acts as a resource and repository for cybersecurity information. The escalation process for attempted attacks should be clear and easily accessible, as should information on the proper use of the company email systems.

III.iii Process improvement

Greater automation, with less manual touch, greatly mitigates the risk of internal fraud but increases vulnerability to cybercrime as more information and transactions are electronic, digitised and web- or cloud-based. Processes should be reviewed and re-designed (if necessary) at least annually to ensure the latest fraud prevention techniques and technology are incorporated into the process and procedures.

Particular attention should be paid to the Procure-to-Pay process since most cybercrime has been directed at fraudulent payments. This starts with the procurement process. Ensuring software and other technology partners maintain robust cybercrime security practices is critical before entering into a contract – and the procurement team should ensure the purchase or service agreement includes adequate language about cybercrime prevention, roles and responsibilities.

Protecting the supplier’s banking and account information is important to prevent payments being directed to a fraudulent entity. Access to vendor master data should be restricted to a dedicated team responsible for vendor master set-up and management. All changes to vendor master data,

Culture

Create a culture where responsibility for mitigating cybercrime risk is shared throughout the organisation

Enforce cybersecurity messaging from the top down

Encourage employees to question suspicious activity

Build and maintain a site of security information, procedures and updates
regardless of how the request is sent in, should be verified by calling the vendor using the contact information originally stored in the vendor master module.

As much corporate spend (both direct and indirect) should be centralised both organisationally and technologically. A centralised team that oversees the purchasing process is vital to ensure purchase requests are legitimate and made according to procedures. Using a web-based portal to manage the purchasing process with verified suppliers is considered a best practice. The purchase requests can be automatically routed to the correct approver based on policy. Final approval triggers the creation of the purchase order that can be sent electronically to the vendor. Requiring a purchase order for all purchases allows an organisation to complete a three-way match between what was ordered, what was received and what was invoiced. This three way match is very important in preventing unauthorised payments.

The actual payment step in the Procure-to-Pay cycle should be monitored closely. There should be clear segregation of duties between who can request, approve and execute a payment. Dual approvals (or more) are considered safer than a single approver. Payments facilitated through SWIFT in XML format are still considered the most secure despite recent attacks on SWIFT service bureaus. Consider 3SKey as an efficient and secure 2 Factor Authentication, an effective way to prevent fraudulent payment initiation

<table>
<thead>
<tr>
<th>Process</th>
<th>2 Factor Authentication, an effective way to prevent fraudulent payment initiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use different passwords for different systems – change them regularly and delete inactive accounts</td>
<td>Require two-factor authentication for payment release (based on a physical or software app token)</td>
</tr>
<tr>
<td>Ensure segregation of accounts by function and payment type, e.g. payroll, claims, and payment volumes</td>
<td>Require dual system-enforced approval for all payment execution exceeding a set value</td>
</tr>
<tr>
<td>Ensure proper segregation of duties between payment creation, approval and release</td>
<td>Monitor and reconcile payment accounts daily: the more carefully accounts are checked, the easier to identify irregular activity</td>
</tr>
<tr>
<td>Implement job rotation and mandatory vacation for payment officers</td>
<td>Implement ‘out-of-band’ transaction notifications for high volume wires and require a second level of authentication</td>
</tr>
<tr>
<td>Maintain a white list of accounts authorised to receive payments – with changes to the list be validated via a dual control</td>
<td></td>
</tr>
</tbody>
</table>
way to authenticate transactions across multiple banks. Reconcile all payments daily to spot any irregularities immediately. Limit the use of mobile payment apps as these can be easily penetrated if not on a secure wifi network.

Always be suspicious of wire requests that are sent with a sense of secrecy and urgency as mentioned earlier. Do not hit “reply” to respond to an emailed payment request. Instead, call the sender or create a new email to the sender to verify its authenticity. Consider having multiple layers of approval. One way to check the authenticity is to hit the reply button (do not hit “send”) and then hover over the email address. Many times the email address is not, in fact, an internal email address but a fake one created by fraudsters. Be aware that fraudsters can gain a wealth of information about the roles of various people within your organisation and may even know when key payment processors are out of the office. More attempts occur on the days leading up to a holiday weekend when back-up staff may be processing payments and may be less familiar with cybercrime prevention steps. Therefore, it is critical to cross-train staff and ensure interns, contractors or temporary staff are equally trained in cybercrime prevention.

III.iv Staff training and awareness
As stated above, personnel is just as important a control for companies against fraud as technology. However, as we have seen, without proper training and cybersecurity awareness – far from helping to guard against a security breach – staff may, in fact, themselves unwittingly cause serious breaches, which can be fatal to a corporate’s defences. Therefore, a C-suite mandate prioritising and emphasising the importance of staff education about, alertness concerning, and responsibility for, inadvertent security leaks (as well as for fraudulent behaviour) is of paramount importance in the fight against cybercrime.

Once the appropriate governance structure and processes are in place, employees need to be trained on these procedures to ensure they are followed. Prevention is key, and no fraud prevention program will be successful if employees cannot detect fraudulent activity and know how to respond appropriately. General cybercrime awareness training should be completed at least annually by all employees, interns and all contract and temporary labourers. Duty-specific training should be conducted for certain teams based on their role in the organisation and their use and access to sensitive data or assets.

Given the ubiquity of business email compromise-related (BEC) attacks, all employees should be well trained on email usage. Only work-related communication and transactions should be conducted over email. No personal use of the company’s email system. Never open any links or attachments in suspicious email. Never send passwords or other credentials via email, text message, or chat. Never trust an email asking you to send money. Follow the process and procedures to all payment requests. Send suspicious emails to IT for diagnostic purposes. Send test emails to employees to gauge the effectiveness of email training and target additional training as needed. Ensure employees know to never use unsecure wifi networks when logging in remotely.

---

**Staff training and awareness**

- Establish and regularly refresh cybersecurity awareness training for all employees
- Execute social engineering fraud rehearsals, e.g. by simulating phishing, smishing, vishing, fake president attacks, etc. to see how employees react.
- Consider incentivising a proactive cyberfraud-aware culture by rewarding employees that detect vulnerabilities and report attacks.
- Distribute the latest fraud trends and protection advisory regularly
Another key area for general training relates to the use of computers and other hardware. Ensure employees are trained to understand that only the IT department can facilitate software downloads on laptops and other devices provided by the organisation. Disable the USB, CD and other ports to add a layer of protection on the device. Or, if USB ports are needed, have IT supply employees with scanned, safe and secure external storage devices. All hardware should require dual authentication, frequent password resetting and “strong” password requirements (at least 8 alpha numeric characters). VPN, tokenisation and encryption are critical. However, encryption alone will not solve the problem. Passwords and other log in credentials should never be shared among employees. Do not allow “bring your own device” for corporate communications unless strong encryption software is loaded. Limit access to sensitive data and systems to only those employees who need access.

However, the second stage of fraud detection and obstruction is equally important and requires effective malware detection software, amongst other tools. Fraud systems are designed to analyse and self-learn patterns in order to detect fraud and stop it when it slips past the initial preventative measures. This technology has been augmented by the use of Big Data as a tool for identifying anomalous or abnormal patterns indicating suspicious activity.

Employing – and maintaining with updates and patches – the latest cybersecurity software is a critical best practice. Ensure detection systems are in place. Work with security technology partners to perform periodic risk assessments and test existing systems for weak access points and remedy as needed. The technology solution should directly align with the policies and procedures in place. If a disparate and disjointed prevention and detection system is in place, consider working with a provider that can link these systems to better manage one large technology program.

For systems and software, ensure the latest anti-virus and anti-malware updates and patches are installed. Intrusion detection systems are a critical step in containing attacks. Have a redundancy plan in case of a dedicated denial of service (DDoS) attack. Encrypt all sensitive data at rest and in transit. Ensure firewalls are in place between distinct networks. Consider establishing separate networks, servers, LANs for different parts of your organisation to limit the impact of a successful intrusion. When using third party partners, always maintain control.
of the data, especially with offshore data storage services. Never allow employees to download freeware, shareware or any other software on a device that is linked to or accesses the overall network or system.

Bank interfaces and other Treasury connections are especially sensitive and should be deeply evaluated. Rationalising bank relationships and bank accounts is a first step in minimising the access points that can be attractive to fraudsters. Consider a 3SKey solution for efficient and standardised communication with your bank partners. Despite recent news headlines, SWIFT and XML format are still considered the safest and most efficient way to send payments.

Consider a separate, dedicated terminal for your treasury workstation that is contained to its own network and server. Always contact your bank representative if you are asked to update bank software or log on credentials via email or via the web.

Freeware

Never allow employees to download freeware, shareware or any other software.

Technology

- Don’t open spam, click on links, or open attachments; delete unsolicited e-mails from unknown parties immediately. These often contain malware that will give criminals access to your computer system.

- Use the “Forward” option to respond to business e-mails, not “Reply”. Either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.

- Ensure your computer has the latest malware protection and anti-virus software installed and updated.

- Consider using high-level macro security settings in software applications.

- Avoid downloading programmes from unknown sources, particularly from the internet and USB sticks.

- Consider using a separate computer dedicated to making online payments with special physical security controls.
IV. The Future of Cybersecurity

**Tomorrow’s threats**
The cost of cybercrime will continue to increase as more processes, corporates and consumers globally go online, with the cost of an average data breach expected to exceed $150 million by 2020.\(^\text{12}\) For corporates, this means higher levels of, and more sophisticated attempts at, payment fraud, extortion and corporate espionage, amongst the many other cybercrimes occurring. But we may also see adaptations of current crimes springing from possibilities yet to be created by future technological developments as well as from the more widespread and integrated application of current technologies.

**Tomorrow’s defences**
Regulation, as well as more standardised and collaborative attempts to combat cyberthreats, is likely to increase as policymakers better understand and acknowledge this problem – and its potential effect on citizens, businesses and economies – going forward. Security in the future will likely be approached via a combination of risk-based and control-based models, with the balance partly dependent on regional risk appetite.

Turning to the tools available for individuals and corporates, we are likely to see significant further advances in both prevention and detection, particularly with regards to ensuring that an authorised individual is carrying out an authorised activity. To this end, we will see greater utilisation of nascent technologies such as biometrics and risk-based authentication.

In particular, there is growing momentum for using handheld devices as separate channels for out-of-band authentication, which allow a transaction to be visualized and authorized via a separate channel e.g. a mobile phone. Such methods of authentication might include voice or facial recognition (e.g. via ‘selfies’), fingerprints, iris or finger-vein/blood-flow scanning – or a combination of factors as in the password-free, 50-factor smartphone security trialled by Deutsche Bank in conjunction with tech firm Callsign, which considers user-behaviour factors such as location and pinpad pressure.

All this will be introduced against a background of increased utilisation of Big Data-driven fraud detection systems which will flag up unexpected changes in patterns of activity. For example, real-time scoring of online usage detects a payment request, for which the user has authenticated himself using two factors (say a PIN + a one-time password), but which is in some way unusual – for example the user’s IP address has suddenly changed. It therefore asks the user

for facial recognition as an additional means of authentication.

It is also likely that, in order to combat social engineering, suspicious transactions will require step-up authentication from the usual four-eye authorisation to a third or fourth authoriser to enable a payment to go ahead, possibly using an out-of-band notification to the relevant manager’s smartphone.

In addition, the development of tools such as Distributed Ledger technology could be used to strengthen protection against cyberfraud. For example, the nature of blockchain means that it authenticates participants and verifies all counterparty identities and can protect consumers and corporates from fraud.

**Conclusion**

Corporates cannot afford to hold back on cybersecurity – they need to prioritise and invest in it now. Taking a more holistic approach influences the success of the cybersecurity program. While technological defences remain crucial, we shall increasingly see employees being the unwitting agents of cyberattacks, unless we educate them in how to prevent attacks – that way, they become instrumental in mitigating cyberrisk. It is the C-suite’s responsibility in every organisation to develop a governance structure and risk culture that elevates the importance of cybercrime. Senior leadership must also ensure that all employees receive the necessary education and training to equip them to understand, be vigilant for and guard against these attacks, and to keep this knowledge and awareness fresh and up-to-date.

As well as thus building and reinforcing their human firewall, corporates may leverage the advice and support of their banking provider to maintain and consistently update both their fraud detection and prevention set-ups, and their cybersecurity tactics as a whole. That way, they have the best chance of eluding a shifting – and ever more slippery and dangerous – web of cyberthreats.
Contact
Pedro Tornero
pedro.tornero@db.com
+49(69)91061295

Ingrid Lauterbach
ingrid.lauterbach@db.com
+49(69)910-67002

Andreas Avato
andreas.avato@db.com
+49(69)910-61037

This brochure is for information purposes only and is designed to serve as a general overview regarding the services of Deutsche Bank AG, any of its branches and affiliates. The general description in this brochure relates to services offered by the Global Transaction Banking of Deutsche Bank AG, any of its branches and affiliates to customers as of October 2016, which may be subject to change in the future. This brochure and the general description of the services are in their nature only illustrative, do neither explicitly nor implicitly make an offer and therefore do not contain or cannot result in any contractual or non-contractual obligation or liability of Deutsche Bank AG, any of its branches or affiliates.

Deutsche Bank AG is authorised under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin)) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorisation and supervision by these authorities are available on request. This communication has been approved and/or communicated by Deutsche Bank Group. Products or services referenced in this communication are provided by Deutsche Bank AG or by its subsidiaries and/or affiliates in accordance with appropriate local legislation and regulation. For more information http://www.db.com

Copyright© October 2016 Deutsche Bank AG.

All rights reserved.