FI Observer – Social engineering – avoiding the hacker's harpoon and phishing net

Social engineering fraud against financial institutions is on the rise globally. What steps should you take to protect your company and will your insurance respond if you suffer a loss?

Social engineering fraud against financial institutions is on the rise globally. Also known as fraudulent inducement, the scams are becoming increasingly sophisticated and the financial and reputational consequences for a company that falls victim can be severe.

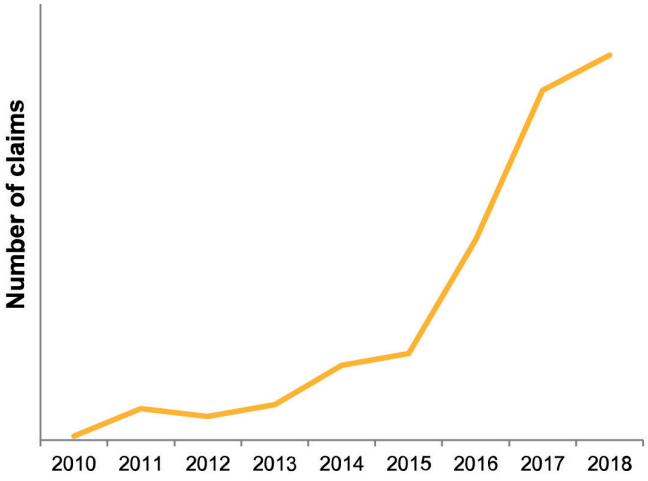
What steps should you take to protect your company and will your insurance respond if you suffer a loss?

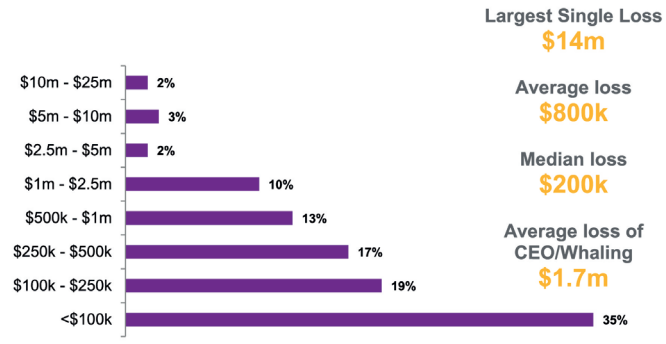
Introduction

The FBI has released a public service announcement stating that between October 2013 and May 2018, the total known worldwide losses to Business Email Compromise ("BEC") scams has now exceeded $12.5 billion. This is a 136% increase in identified global exposed losses between December 2016 and May 2018. We know from the announcement that the fraudulent transfers were sent to 116 countries with the majority going to Asian banks located in China and Hong Kong. However, financial institutions in the UK, Mexico and Turkey have also been identified recently as prominent destinations.

Social engineering fraud involves criminals exploiting unsuspecting employees into transferring money (even other assets too) or key confidential information to them, usually for financial gain. Attacks are increasing in volume and scale and all financial institutions, large and small, are at risk of suffering significant financial losses.

This increase can also be seen by the upturn of social engineering claims that Willis Towers Watson has notified to insurance carriers on behalf of clients, with 2018 being a record year.





Willis Towers Watson

What is social engineering?

Social engineering can take many different forms. You may be familiar with terms such as “phishing”, “baiting” or “fake president” scams. These scams rely on the perceived weakness in any company – its employees. The scams operate by criminals exploiting certain qualities in human nature, in particular trust and the desire to be helpful, to deceive employees into breaking normal security procedures and providing company information or transferring funds to them.

Nowadays fraudsters are using increasingly sophisticated and targeted methods to defraud companies. This can involve, for example, hacking into a company’s databases (often undetected) and trawling through internal information for many months in order to construct a convincing scam.

Phishing: Sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers

Whale Phishing: Targeting specific high ranking individuals in the company

Baiting: Leaving an innocent looking, but actually malware-infected device e.g. a USB drive, somewhere where an employee will find it and out of curiosity plug the infected device into their computer

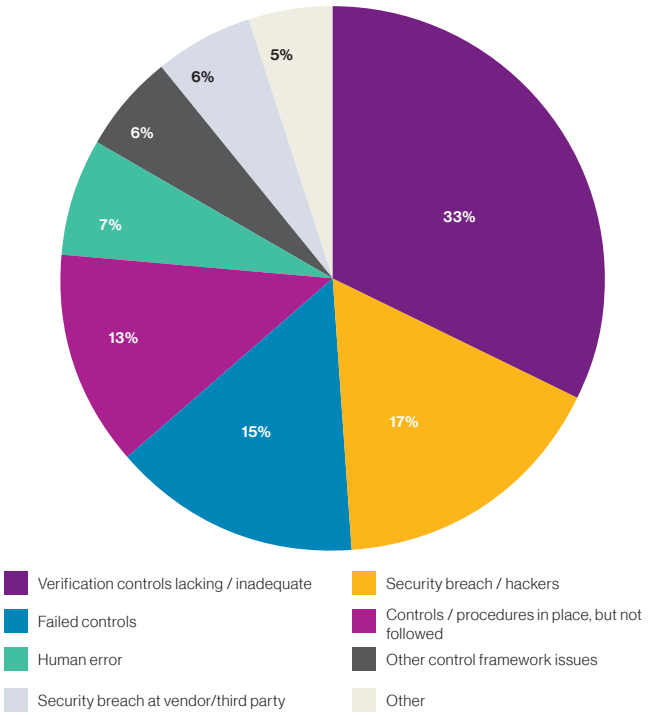
Fake president / CEO fraud / business email compromise: Targeting employees with access to company finances and tricking them into making money transfers to the bank accounts of the fraudster. Often the fraudster, having gained access to the company’s computer system, will send an urgent email pretending to be the CEO/high ranking executive in the company, a vendor or a trusted customer.

How does it happen?

Security experts recognise that most social engineering scams follow a four-stage process: (1) information gathering (2) relationship development (3) exploitation and (4) execution.

91% of cyber-attacks start with a phishing email[1]. The email will usually have a message requiring the individual to click on a link or an attached file, which will give the attacker access to the computer network and possibly unleash computer malware into the company’s network. Once in the network, the attacker can spend months unnoticed residing in a company’s computer system perusing emails, recording key strokes, and learning about protocols, writing styles of people they want to impersonate and confidential information about pending transactions or deals requiring a material fund transfer. Therefore, when a person receives an email or phone call from a fraudster impersonating a person in authority at the company or client, it is often hard to know they are falling victim to a criminal act and being duped into transferring funds into a fraudulent bank account.

The email request will likely be packed with confidential or private information that no one but the purported sender would know, thereby lending the communication instant credibility. Often the email will be sent at an exceedingly busy time or late in the day and may include some seemingly valid reasons why normal authentication measures should not be followed or deviated from. These emails often have great urgency associated with sending funds, where failure to do so immediately would apparently have significant consequences for the company, leaving the recipient in a highly uncomfortable position of actioning the transfer without the ability to properly authenticate it - or to not send it and risk the consequences for not completing the transaction.



First line of defence – internal controls

The first defence for any company is deploying robust internal prevention techniques to recognise and deflect social engineering attempts. Some self-protection strategies that can be adopted, by way of example, are:

- **Verify changes** in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- **Confirm requests** for transfers of funds. When using phone verification as part of the two-factor authentication process, use previously known numbers, not the numbers provided in the email request.
- **Know your customer.** Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- **Beware sudden changes** in business practices e.g. a request by a business partner to be contacted via a different channel – verify through other channels you are still communicating with your legitimate business partner.

1. PhishMe report

- Carefully **scrutinise all email requests** requesting transfer of funds to determine if the requests are out of the ordinary.
- **Create intrusion detection system** rules that flag emails with extensions that are similar to company email. For example, legitimate email of abc_company.com would flag fraudulent email of abc-company.com.
- **Report and delete unsolicited email (spam)** from unknown parties; do not open spam email, click on links or open attachments.

The weakest link

Even if a company does have good protocols in place to prevent fraudulent activity (such as per the above), the human element risk means that it may still be vulnerable. Therefore the best defence for combating social engineering fraud is awareness through corporate culture, education and training. Companies with an increased awareness and understanding of social engineering scams are more likely to recognise when they have been targeted by fraudsters, and are therefore better equipped to avoid falling victim and sending fraudulent payments.

Therefore, appropriate training at all levels (especially targeting front-line employees who may be the recipients of initial phishing attempts) is critical for protecting your company. Like any good security measure, it should be continually updated as new trends emerge.

Insurance / risk transfer

If, for whatever reason, criminals are successful in engineering a fraud, is there anything you can do to recover the loss? Generally, it can be very difficult to recover lost funds, particularly if there is a time delay before the company becomes aware that it has been compromised. In these circumstances, insurance cover can be key.

Crime policy cover

Insurance coverage for social engineering losses differs from policy to policy. To the extent that cover is not already provided by the policy (usually within broad computer crime wording), it can be added via a social engineering extension, which includes two important elements of cover:

- **Fraudulent transfer instruction:** Typically refers to fraudulent emails or phone calls purportedly sent or communicated by a customer, an employee acting on behalf of the customer or another financial institution acting on behalf of the customer, instructing the financial institution to transfer customer funds under its care, custody and control
- **Impersonation fraud:** Covers fraudulent vendor and employee or officer requests and most often refers to the financial institution's own funds; not those of a customer.

As the position varies from insurer to insurer and across jurisdictions, care should be taken to review the extent to which this extension dovetails with other coverage provisions.

Recent US cases

In the US, recent high-profile appellate court decisions, Medidata and American Tooling Center[2], seemingly provided hope to policyholders looking to secure social engineering cover under standard, unendorsed crime policy forms. However, the celebrations were short lived. First, it should be noted that the underlying policies in both cases were commercial crime policies, not financial institution crime (bond) policies. Second, following these rulings, insurers quickly amended policy terms and removed whatever element of social engineering cover may arguably have existed in base, unendorsed policies. **Therefore, inclusion of a social engineering policy extension remains the safest option.**

While it was more common for this type of cover to be sub-limited in the past, particularly in the US, it is now more usual for insurers to make full policy limits available for social engineering losses, after some additional underwriting (see below). This is particularly beneficial to financial institutions given the trend we are seeing in the increasing frequency and severity of these frauds.

UK and US underwriting

Some policies in the UK, with respect to cover found under a social engineering extension may be conditional upon the financial institution having written policies/procedures in place for authenticating a payment or transfer request and being able to reasonably demonstrate, in normal circumstances, that such written policies and/or procedures are followed (or a variant thereto). While insurers may not prescribe what the specific procedures should be, underwriters will ordinarily require a detailed description of a company's protocols and procedures before agreeing to underwrite social engineering risks.

In the US, certain markets have expressed flexibility as to the nature of the anti-fraud policies and procedures specified in their policies. While some markets still condition coverage on a rigid set of procedures (such as call backs) which may or may not be relevant to a firm's particular anti-fraud regime, others now include "catch all" language in their policies. This coverage enhancement allows a financial firm to design and implement its own anti-fraud regime and then seek the carrier's consent to integrate those policies and procedures into the policy's coverage preconditions.

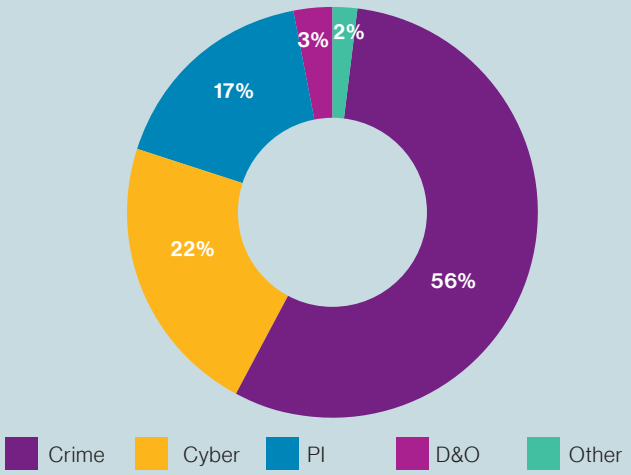
Civil liability (UK) policy

Whilst crime policies can cover direct loss of funds, a Civil Liability policy may also be engaged in the event of a social engineering fraud where an allegation of negligence is brought against the company arising out of its provision of services (or lack thereof) to the customer.

2. American Tooling Center, Inc. v Travelers Casualty and Surety Co. of America, No. 17-2014, 2018 WL 3404708 (6th Cir. July 13, 2018)

Cyber policy

While social engineering frauds are often orchestrated via email, the losses are typically covered by a crime policy rather than a cyber policy. Cyber policies tend to cover losses resulting from unauthorised data breaches or system failures, both impacting information as opposed to money/ other assets. For example, cyber cover might include management of a breach and costs associated with hiring experts such as IT forensic experts to investigate the breach and effect repairs; legal experts, with specialist experience in the privacy/regulatory arena; or crisis communication consultants to minimise reputational damage.



Conclusion

As the risk of social engineering fraud continues to rise, financial institutions should ensure they have effective protocols and procedures in place to avoid becoming another social engineering statistic. Employee awareness through corporate culture, education and training is also vitally important.

In order to benefit from social engineering insurance coverage, companies need to demonstrate to insurers that they have robust protocols in place to prevent social engineering fraud. Having effective insurance cover in place completes the circle of effective risk management, to cover the company in the event that it does fall victim to a fraud. There will always be criminals that slip through a company's 'phishing net'. However, the key to effective risk management are protocols, training and customized insurance.

For further information please contact:

Claire Nightingale
+44 20 3124 6928
Claire.Nightingale@WillisTowersWatson.com

Anthony Rapa
Anthony.Rapa@WillisTowersWatson.com
+1 212-915-8506

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

Willis Limited. Registered number: 181116 England and Wales.
Registered address: 51 Lime Street, London, EC3M 7DQ.
A Lloyd's Broker. Authorised and regulated by the Financial Conduct Authority for its general insurance mediation activities only.

willistowerswatson.com

Willis Towers Watson