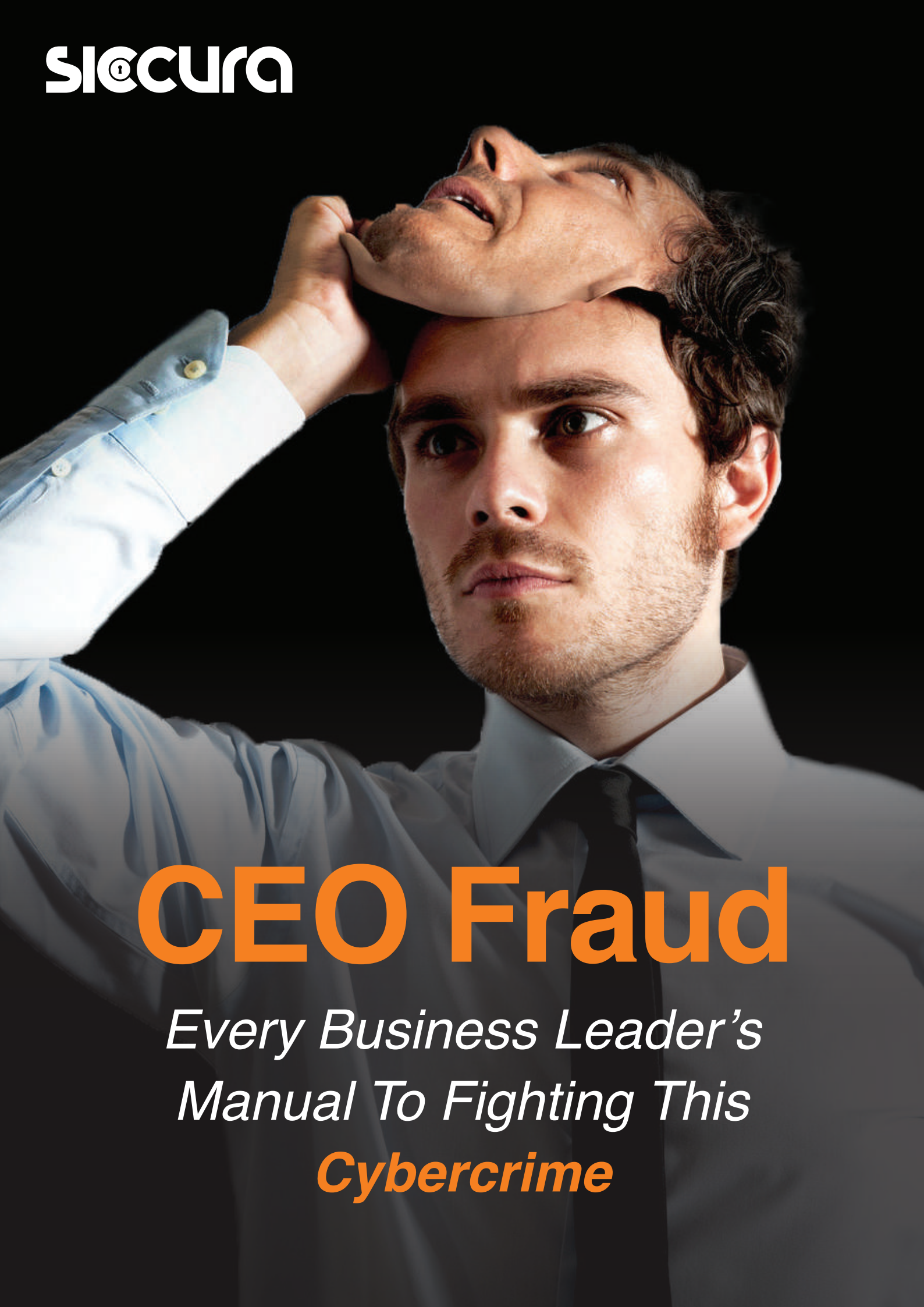
siecura



CEO Fraud

Every Business Leader's Manual To Fighting This ***Cybercrime***

CONTENTS

PART A: INTRODUCTION

It's 6am on Monday, and you've just got out of bed to start a new working week. After a shower and a quick breakfast, you make a run for the train. As you board the usual crowded train, you start to look at your phone, the usual emails come through- and then you spot an email saying "Urgent Transfer". It's from the CEO. You're immediate reaction is excitement (because he doesn't even know you exist) and what could he possibly want with the Junior accountant.

As you read through the email trail, you notice that Clive, your boss has been copied into it. With Clive on a 2 week holiday in Malta, and the boss asking for an urgent transfer- that's the first thing you've got to do when you get into the office.

Only three more stops before you've reached your destination. You rush into the office, and before you take your first cup of office coffee you make the transfer. Phew! The boss will be pleased. Your quick reaction, commitment is bound to get you that promotion.

A few days later Clive calls you asking why $250,000 had been transferred. That's when you realise that you've been scammed. It turns out that you've been involved in a CEO Fraud incident. The email was not from the CEO, and Clive hadn't even received the copy of the email as it was spoofed. This incident is under investigation. There's nothing you can do apart from pray that the money can be recovered.

This is an all too familiar story of CEO Fraud. According to the FBI's Internet Crime Compliant Center (IC3), CEO Fraud is continuously growing. Though the number of CEO Fraud scams have been increased, the heightened awareness of this type of scam has contributed in an increase on the number of attacks being reported. Awareness and knowing how to combat this crime.

This CEO Fraud Guide provides an in depth overview of how to deal with this rapidly growing wave of cybercrime. This guide will give you an understanding of this type of attack, put you into the mind set of cybercriminals, and how to prevent your business from falling victim.

PART B: UNDERSTANDING CEO FRAUD

What Is CEO Fraud?

CEO Fraud, also known as Business Email Compromise (BEC) is one of the most financially damaging types of cybercrime around. Over the years it has victimised more than ***78,617 organisations globally,*** and is responsible for the loss of ***over $12.5billion*** (£9.6million) since May 2018. No doubt this figure will only increase. This type of online crime has ruined many executi ves and employees careers. CEOs have lost their job and position because of it. Stock prices have collapsed. IPOs or company mergers have been halted as a consequence. So what exactly is CEO Fraud?

The FBI defines it as “sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds.”

CEO Fraud is a form of spear phishing where cybercriminals impersonate the CEO or any high authority position of a company. They impersonate the C-Level positions to trick employees into carrying out actions that risk company data or credentials. The core of every CEO Fraud attack is MONEY. CEO Fraud attacks are designed to trick employees into moving money from the company’s bank account into scammer’s account.
CEO Fraud attacks are often appear in four methods. It’s important for Business owners to stay on top and understand exactly how this crime is committed.

Types Of CEO Fraud Attacks

To understand CEO Fraud, and stand a chance of combatting this type of attack, business leaders need to understand the four methods cybercriminals use.

Phishing

Phishing emails are sent out in masses to a number of people in an attempt to “fish” for sensitive information by posing as a reputable source. Phishing attacks commonly disguise itself as Banks, Credit card providers, delivery firms, law enforcement, government or health authorities. Phishing emails often have legitimate looking logos attached.

A typical Phishing campaign means shooting out emails to a huge number of users. However, most of the people that these attacks go to do not have any association with the company it has disguised itself as. But given the weight in numbers, these emails eventually do arrive to a certain percentage of likely candidates.

Spear Phishing

Spear Phishing is a much more focused type of phishing attack. This type of attack targets a specific organisation or individual to get access to their sensitive information. Behind every Spear phishing attack, the cybercriminal has done their homework on the target. Unlike spam, Spear Phishing attacks appear to come from trusted and known sources.

The email generally goes to one person or a small group of people who use that bank or service. As the cybercriminal has studied the target, the email will be personalised, and include the person's name or the name of the client the target is associated with.

Executive "Whaling"

As the name states, this type of attack involves the cyber criminal going for the bigger fish in the company - that's the top executive and administrators in order to steal money or confidential data. As high level positions have the most access to critical information, this makes them natural targets. Similar to a Spear Phishing attack, the cybercriminal will study the target to ensure that the email delivered is personalised.

Social Engineering

All of the techniques mentioned above fall under the category of Social engineering. Social engineering is the art of manipulating, influencing, or deceiving someone in order to gain confidential information or money. To deceive the target, cybercriminals mine for information from social media sites, LinkedIn and Facebook profiles, and other sites will provide a wealth of information about the organisation's personnel. The type of information that can be found includes contact information, connections, friends and details of ongoing business deals, photos and more.

What Is The Difference Between Whaling And CEO Fraud?

Whaling and CEO Fraud may look identical but are far from it. For a start Whaling attacks target the big fish –the top level executive such as the CEO to get the confidential information in order to hold them ransom. Whaling attacks have seen a sharp rise and are expected to continue to rise up. In 2018, the FBI reported a loss of more than $12.5 billion as a result of Whaling attacks.

CEO Fraud on the other hand uses senior level executives to exploit other employees within the organisation.

Unfortunately, many of these attacks have a high success rate. 30% of recipients open a phishing message and 12% click on attachments. Many of these breaches happen within 2 minutes of receiving the email. That means the IT department have slim chance of catching the malicious attack before it hits inboxes.

How Does CEO Fraud Work?

As the old saying goes, to catch a criminal, you need to think like one. We know that the core of every CEO fraud is money. The cybercriminal's motive is purely to move money from one account into their account. How they do this is like this:

Know Your Target

It all starts with knowing your target. Cybercriminals will start to mine for information about the company, and business partners associated with the target. As CEO Fraud scams require a degree of trust, they often use existing relationships to propagate the crime.
For example, relationships revolving around the CEO of the company. Cybercriminals will research into understanding the relationship employees and partners have with the CEO.

As CEO Fraud involves disguising communications to make them appear like they are coming from the CEO the attacker will determine if the CEO or executive's domain can be spoofed.

To see what information can be extracted, cybercriminals will send out spear phishing emails to the target into revealing login details.

Start Socialising

The success of a CEO fraud depends on tricking the human being. The best way to do this is to “groom” the individual by using trust. The person that they usually choose is someone in the accounts department who can make transfers.

The Attack

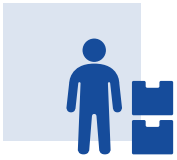
Once the Cybercriminal has everything she/he needs, they will go for the attack. The attack usually involves an email being sent to the target asking for a transfer.

Time To Cash In

The Cybercriminal cashes in the funds without the company suspecting.

Though Cybercriminals are becoming sophisticated day by day, and using different tricks to convince us. There are 5 common attack scenarios that Cybercriminals will use in a CEO Fraud scam.

Common Attack Scenarios



Foreign Supplier

This scam takes advantage of the long established relationship with the supplier, but asks for funds to be sent to a different account.

Wire Transfer Requests

This scam usually compromises or spoofs the executive's email account, which is then used to send an employee an urgent message to transfer funds somewhere else. This type of scam appears genuine because it comes from the correct email address.

Fraudulent Correspondence

This attack involves taking over an employee's email account and sending invoices out to the company's suppliers. The money is then transferred into the cyber criminals accounts.

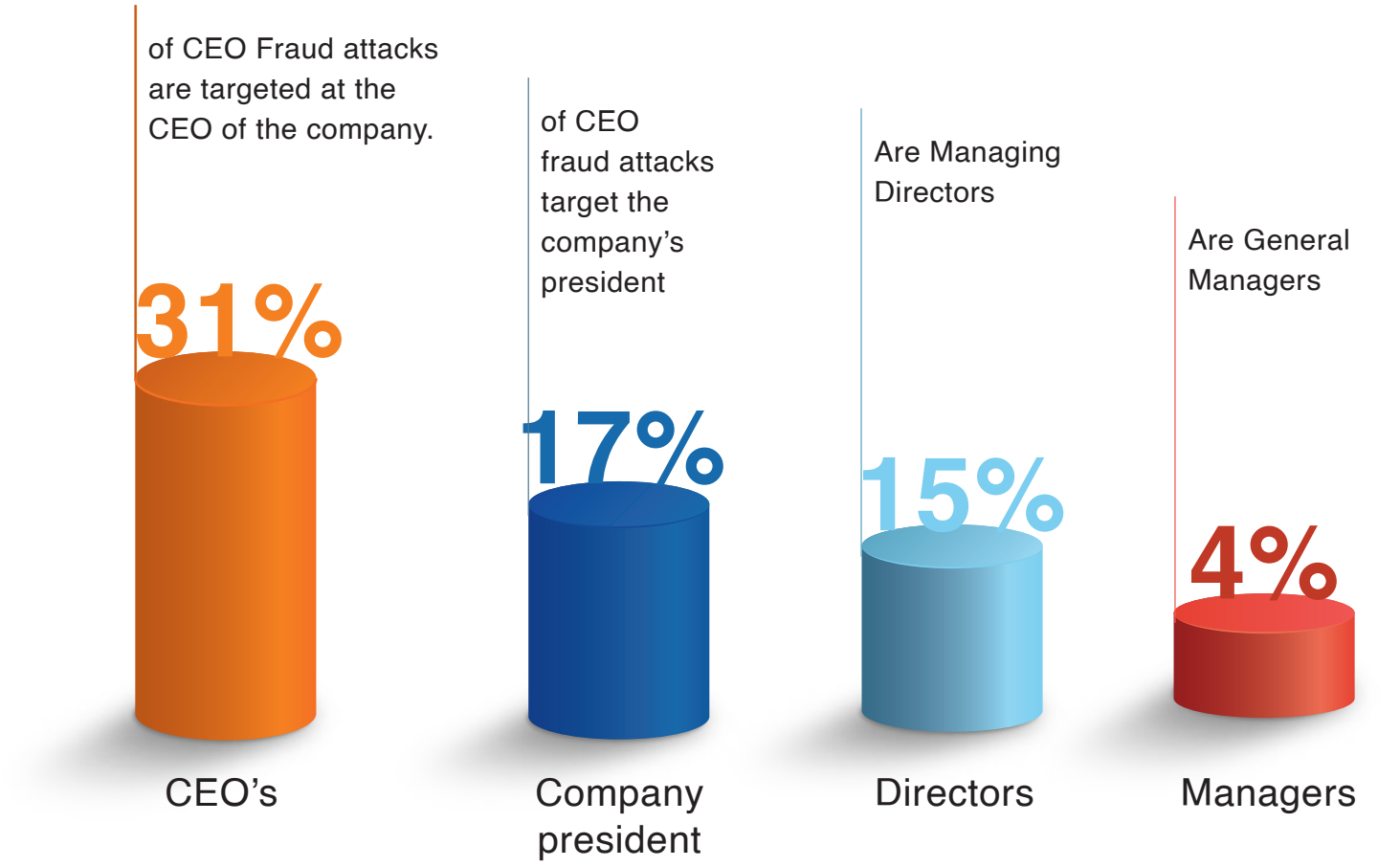
Lawyer Impersonation

The cybercriminals presents themselves as lawyers or executives dealing with confidential and time-sensitive matters.

Data Theft

This attack requests fraudulent emails requesting for salary or tax statement forms of all employees. This attack is sent to HR or accounts departments.

Who Are The Targets?



In terms of departments, the Finance department is vulnerable to CEO fraud attacks as they regularly engage in money transfers. The next group is Human Resources (HR). HR manage the employees' data base and are in charge of recruitment. As a major part of their function involves shifting through resumes, all it takes is a cybercriminal to send a resume containing spyware to surveillance the company.

In addition, the executive team can also be considered a valuable target. Every member of this team possess some kind of financial authority. If their email accounts were hacked, then it would give cybercriminal access to all kinds of confidential data, as well as information about business deals. Surprisingly, IT units are also the hot pick for cybercriminals due to their control over password management and email accounts. If their credentials can be hacked, then they can gain entry to every part of the organisation.

What Damage Can CEO Fraud Do?

CEO Fraud is an expensive threat, and can have a lasting impact on the business. According to a report conducted by UK Banking service Lloyds, nearly half a million SMBs have been affected by CEO fraud. Action Fraud reported that the largest amount ever to be transferred by an employee in a CEO Fraud attack was £18.5million.

Aside from the financial loss, companies can also lose any potential mergers or IPOs from occurring. The ramifications of CEO fraud can also cause the loss of a bid on a large contract, loss of revenue, reputation, and compromise intellectual property (IP).

Real Life Casualties

Norfund

In March 2020, a Norwegian private equity investment firm loss more than $10million as a result of CEO fraud. The theft went undetected until end of April as the cybercriminals had tried to attack the firm again.

Ubiquiti Networks

$46.7 million was stolen as a result of CEO fraud. The Cyber criminal had made contact with one of the company's foreign subsidiary companies and was able to impersonate a C-level executive.

FACC

An Austrian aerospace company lost $61million in a CEO Phishing attack. The phishing email had impersonated the CEO Walter Stephen and was sent to a fairly low-level employee within the accounts team. The email had provided a sense of urgency and a explanation that the funding would be for a new project.

Crelan

The Belgium bank lost $75.8million in a CEO fraud attack. The attack method used was a Wire transfer request, which had gone undetected until an internal audit had flagged up the transfers.

Xoom Corporation

A California based international money transfer Company reported an incident where spoofed emails were sent to the finance team. This resulted in a transfer of $30.8million in corporate cash to fraudulent overseas accounts. Not only did the company suffer from financial loss, but the stock dipped to 14 (approximately $31 million).

Scoular Corporation

The commodities trading firm reported a spear phishing incident involving a wire transfer request. The company's employees received an email claiming to be from the CEO. The email had referenced an acquisition of a business in China asking to transfer the declared amount.

As the email had come from the CEO, the employee did not question it, and had transferred the money. This incident had occurred in 2014, but the FBI had taken further action in 2015. When the money was finally tracked down the account was closed, and the money was transferred somewhere else. To make things even more complicated, the fake email was created in Germany, but the actual email domain was hosted in a server in Russia.

Mattel

The toymaker company based in America became a victim of a very sophisticated phishing email which was directed to a finance executive who was able to approve large transfers. The phishing email had impersonated the newly appointed CEO Christopher Sinclair. The cybercriminals had studiedsenior staff members, and as a result they were able to understand the company structure and payment patterns.

This resulted in luring over $53 million out of Mattel's bank account and into the Bank of Wenzhou, China. Fortunately, the funds had been returned as both banks had been alerted. These are just a few companies that have suffered as a result of CEO Fraud. According to the IC3, CEO fraud scams are continuously evolving, and target businesses of all sizes, including smaller businesses. The ramifications of CEO Fraud have a knock on effect – Reputation, Trust, Careers, and Money are all on the line with this attack. From an individual's perspective, the risk of losing one's job should be enough motive to pay attention to the potential for fraudulent scams. When high-level positions such as CEOs and CFOs have lost their job over a breach – Ignorance is no excuse.

Tackling CEO Fraud is not the sole job of the IT department. It requires the entire organisation to be vigilant as everyone plays a role in this type of attack.

PART C: PREVENTION

Cybersecurity, Malware, and Virus have for too long been viewed as an IT problem. Though some organisations appoint Chief Information Security Officers (CISO), information security is often viewed as a challenge that is not for the board and C-level position.

Companies, no matter the size must take reasonable measures to prevent cyber-incidents and mitigate the impact of breaches. If CEOs and other members of the business do not act now, then it can open the door to legal action. To put things in perspective, a cyber breach can potentially cause the loss of a bid on a large contract, compromise Intellectual Property, loss of revenue and trust. With the stakes so high, this should be enough to put Cybersecurity on top of every organisations agenda. To tackle any type of Cybersecurity incident, everyone in the business needs to be aware.

One Crime – Multiple Names

CEO Fraud. Business Email Compromise (BEC). Bogus Invoice Scheme. Employee Account Compromise. Man-in-the Email Scam. CEO Fraud disguises itself as different names- you need to be aware of them all. To tackle CEO fraud, many steps need to come together in order to create an effective prevention program.

1. Dentify the High-Risk Users

We already know that with this type of attack, it is not just the CEO who is at risk. High- risk users include other C-level executives, HR, Finance and IT staff. Implement more controls in these units. For instance, bank transfer approvals must have different authorisations and a time period before the transfer is executed.

Conduct a search on all the high-risk users in your organisation to see how exposed they are. Look at their LinkedIn and Facebook profiles, as these often contain personal information, or even what could be considered sensitive corporate data such as email address, or a list of connections. If the profiles contain sensitive information, edit those profiles to ensure no personal or business information can be found out.

2. Technology

Even though cybersecurity is more about training people and altering people's behaviours, technology can help. There are various technology controls around which prevent phishing attacks from succeeding.The obvious technical control is email filtering. Authentication measures should be heightened.

Rather than having a simple username and password, implement a two-factor authentication which requires something only the user has on them. Introducing two-factor authentication makes it harder for potential intruders to gain and steal access to someone's personal data or identity.

3. Policy and Procedures

No matter the company size, every business should have a security policy which is regularly reviewed and followed by employees. The security policy should include policies around:

- Not opening attachments and clicking on links from unknown sources
- Not using USB drives on office computers

As part of the policy, there should be a section which covers Password Management, which includes not recycling work passwords on other sites and machines, not displaying passwords on Post-it notes or screens.

Other types of policies include WiFi access, bank transfers and handling confidential data. Policies around bank transfers should never make it

possible for cybercriminals to hijack an email account and convince someone to transfer a large sum of money immediately. These policies need to be thorough and make it impossible for anyone to steal from the company unnoticed.

The same rules should apply when formulating policies around IP or employee records. The policy should involve several approvals before such information is released.

As for Procedures, IT should have various measures in place to block sites known to spread ransomware, or other viruses. Software patches and virus signature files should also be up to date.

There must be procedures to prevent CEO Fraud from occurring. To tie in with the security policy, the procedures must involve the authorisation of multiple people as well as a confirmed email. It should also include Phone, or face to face confirmation, that way the phishing email attack can easily be quashed. To combat the urgency issue that is often portrayed in cyber criminal emails, introduce a standard procedure of a 24 hour waiting period before funds are transferred. This will allow for necessary authorisations and side checks to be completed.

4. Cyber Risk Planning

Though Cybersecurity is considered to be a technology issue, cyber-risk must be addressed and managed at all senior levels. Cyber risk management is a process of identifying, analysing, evaluating and addressing the organisation's cyber risks. It is important for the CEO to be fully aware of this.

When thinking about implementing Cyber risk management into the organi sation, the first step is to do a cyber risk assessment.

A typical risk management programme involves the following steps:

- Identify the risks that compromise the businesses cyber security. This would mean identifying the vulnerabilities in the systems that are used, and threats that might exploit them.

- Analyse the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.

- Evaluate how each risk fits within your risk appetite.

- Prioritise the risks

- Decide how to respond to each risk. Some people might:
  - **Treat** – modify the likelihood and/or impact of the risk.
  - **Tolerate** – make an active decision to retain the risk (e.g. because it falls within the established).
  - **Terminate** – Completely change or end the activity that causes the risk.
  - **Transfer** – Share the risk with another party such as getting insurance.

As cyber threats continue to evolve, monitoring and reviewing plays an essential part in the Cyber risk management programme.

99% Of Cyber-attacks Require Human Intervention

5. Train Your Workforce

No matter what policies, procedures or technical controls you have in place- cyber-attacks are inevitable and rely on human intervention. When 95% of security attacks are successful because cybercriminals prey on human weaknesses, it's time to turn your workforce into front line defenders. Training is a key aspect to the organisation's prevention strategy.

Train staff on the security policy and procedures. To let the information sink in, convert it into handbooks, posters and other visually stimulating materials.

Security Awareness Training

Security awareness training is a must as educating employees will reduce the success rates of attacks. Security awareness training is often accompanied by simulated attacks, which give employees a chance to experience real life CEO fraud attacks. Implementing regular mock attacks will sharpen up employee's behaviour towards these types of emails. Once they realise the repercussions of repeated failures, the attitude changes.

When conducting mock attacks, send different types of emails to different groups of people in the company. This way you will avoid one employee warning others about the mock attack.

Spotting The Signs:

Security awareness training also includes educating people how to watch out for red flags. To catch a phishing attack such as CEO Fraud, watch out for these symptoms.

1. From Field – Do I know the sender? Do I normally communicate with the sender? Is the email from a suspicious domain? If in doubt, don't open it.

2. Attachment – Were you expecting to receive an attachment? Do you normally receive attachments from the sender? What type of file is attached? If in doubt, don't open the attachment.

3. Subject Line – Does the subject line create a sense of urgency? Does the subject line match the email content?

4. Use Of Language – Does it uses phrases such as "Urgent wire transfer", "Urgent invoice payment" or "new account infor mation". Does the email contain obvious spelling or grammatical errors?

5. Hyperlink – Is the test of the link the same as the destination? Does the link include incorrect spelling or modified version of a known URL? If in doubt, do not click on the link. Verify the link by calling the sender.

PART D: RESOLUTION

I Have Been Scammed- Now What?

If a CEO fraud incident takes place in your organisation, then you must take immediate steps.

Contact The Bank

Immediately alert your bank about the fraudulent transaction. They should be able to try to re-call funds.

Contact The Police & File A Complaint

Gather all documents regarding the transaction, email and invoices and contact the police to file a complaint.

Fraudulent Correspondence

This attack involves taking over an employee's email account and sending invoices out to the company's suppliers. The money is then transferred into the cyber criminals accounts.

Brief The Board And Senior Management

Call an emergency meeting with the board and senior management to brief the incident, and any steps that need to be taken further.

Contact Your Insurance Company

Contact the insurance company to find out if you are covered for the attack.

Do IT Forensics

Get the IT unit investigate the breach to look for any open doors. If an executive's email has been hacked, take immediate action to recover control of that account by changing the password.

Review Policy Violations

If the incident occurred that means that there has been a violation in the existing policy. Conduct an internal investigation to see if there has been any violation.

Draw Up A Plan To Remedy Security Deficiencies

Once all consequences have been addressed, and all data has been gathered- the only thing left is to draw up a remedial plan. Look at implementing strategies that will ensure this type of attack does not happen again. Your strategies should focus on increasing security awareness training.

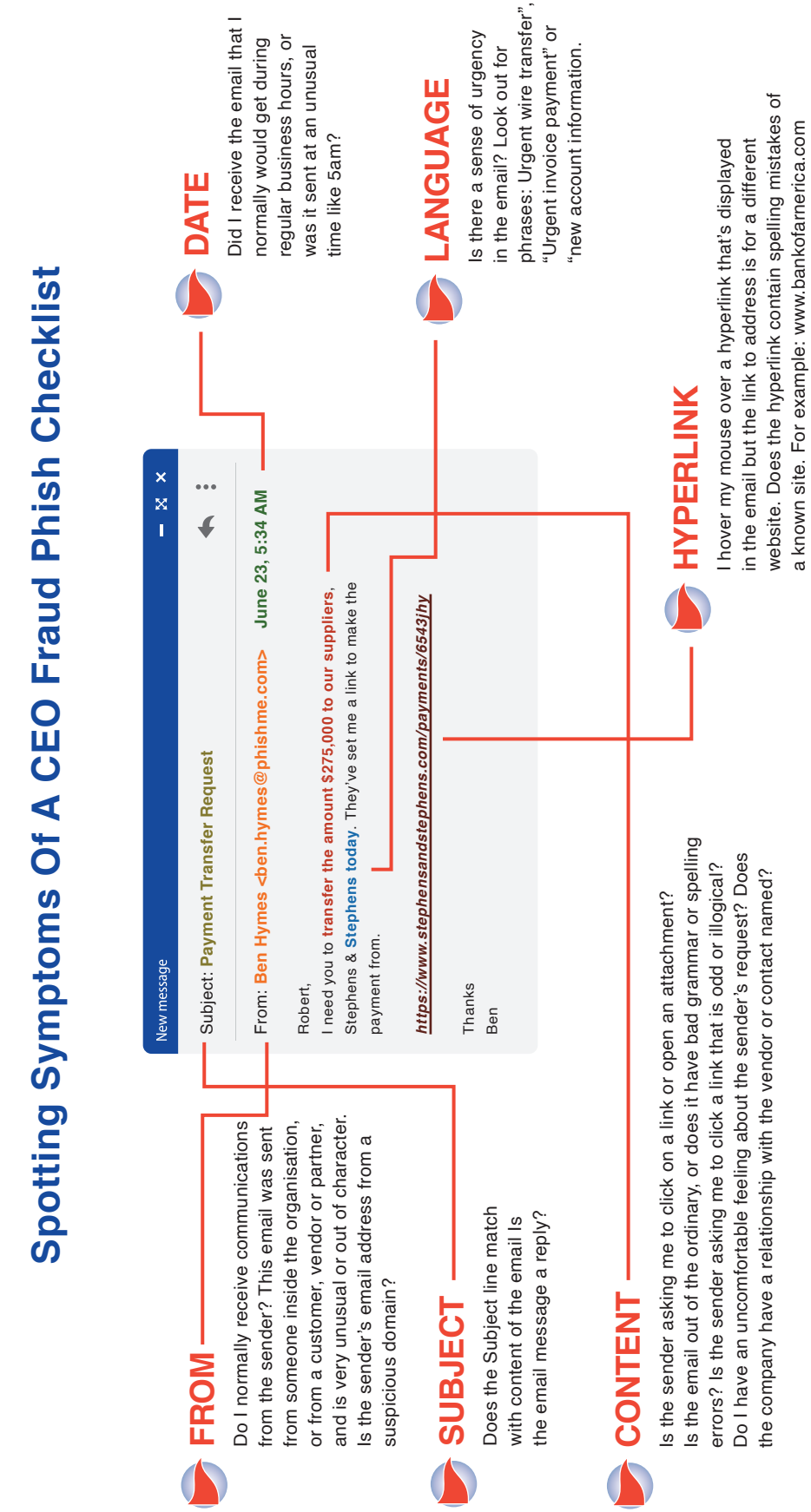
Conclusion

There is no alternative other than preparation when it comes to combatting a cybercrime that has multiple names. CEO Fraud is a crime that will continue to evolve over time. But as it evolves, CEOs and other C-level executives need to take a stand by training their staff into becoming the company's front line defenders.

Testing, increasing awareness, and continuously engaging employees in cybersecurity threats will strengthen any organisation. After all a human cybershield is far more effective than a firewall.

PART E: RESOURCES

The first step to combatting CEO Fraud is learning how to spot the signs. This will give you an idea of what to look out for.



Don’t Get Caught On The HOOK

Be SIccura