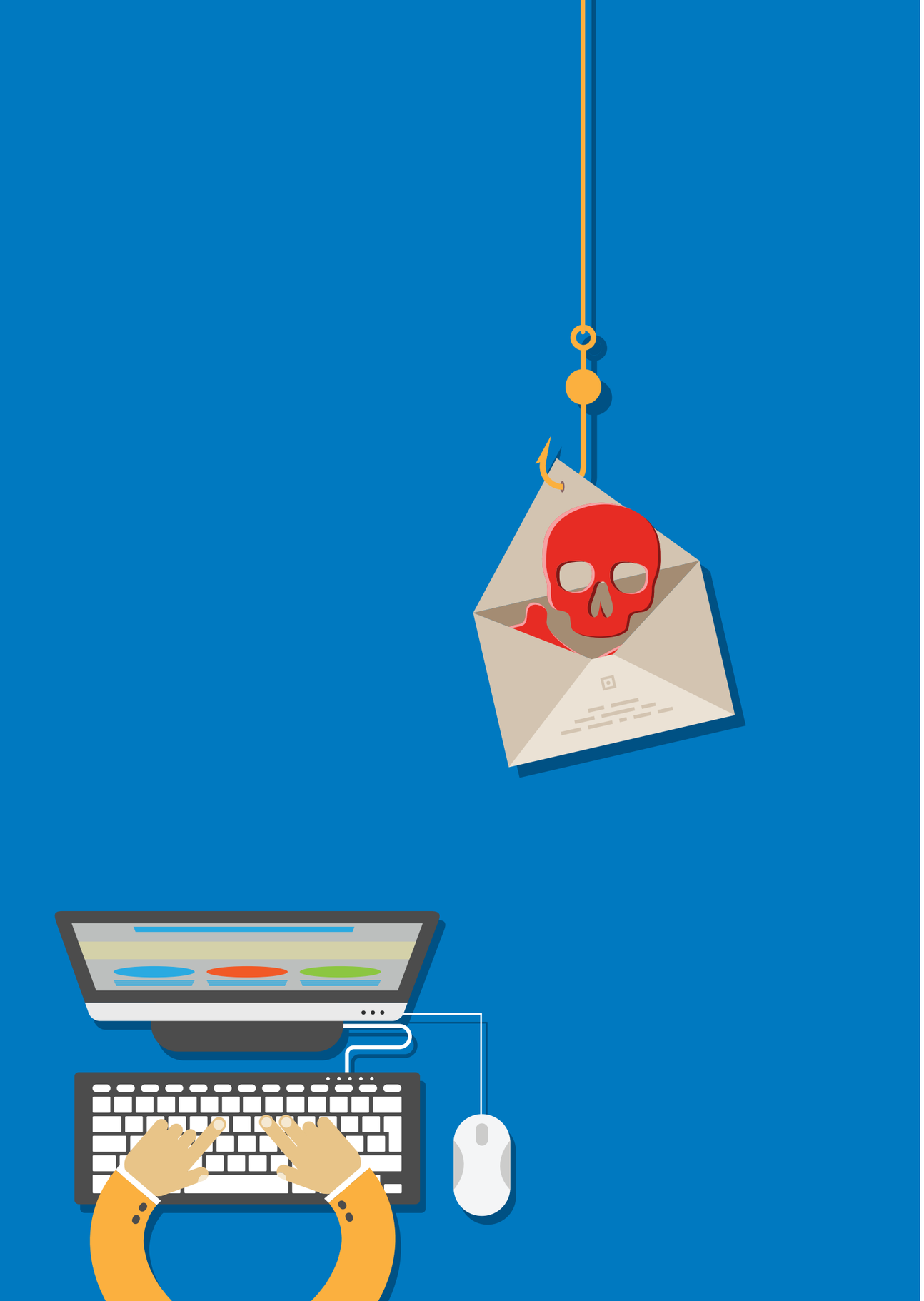
WHITEPAPER

Cyber Risk is a Human Risk

Cyber Risk Aware

Creating your human firewall!



Key Facts/Figures:

Independent research has shown that the cost of a Cyber Attack to an organisation is proportionate to the number of employees, with the average cost estimated at **$395 USD Per Employee – Per Attack .**

From a technical perspective, Cyber Criminals have continued to develop increasingly more sophisticated and complex malware as part of their activities; however - despite this complexity - Cyber Criminals continue to rely on the simplest of mechanisms to deliver malware to their victims: **Phishing E-mails.**

Phishing Attacks are by no means complex; they simply takes advantage of well-known weaknesses and poor behaviour traits of human e-mail recipients and computer users: **Three out of every Ten Phishing E-mails which arrive in the inbox are Opened** by the recipient; **For each Phishing E-mail that is Opened, One in every Eight people either click on an embedded link or download an attachment** (this in itself is enough for a Cyber Attack to take place either via a drive-by-download - in the event of clicking a link - or some form of malicious attachment); **A further One in Eight people proceed to disclose the information requested (or perform the task requested) in a Phishing E-mail** – with this figure rising significantly for more advanced forms of phishing attacks such as Spear Phishing and CEO fraud.

Research has shown that S**pam/Phishing filtering software only has a success rate of 93%.** Given the sheer quantity of Phishing E-mails in circulation at present, this gap of 7% ensures that a significant amount of Phishing E-mails end up in the inbox along with legitimate e-mail - and this is where the danger lies. **1 in every 1,846 e-mails sent globally is a Phishing E-mail;** however certain business sectors, company sizes and employees are targeted more often than others: Companies ranging in size 1 – 1000 employees are 50% more likely to be the target of a Cyber Attack via Phishing in comparison to larger companies (with companies in the 251 – 500 range twice as likely to be the victim of a Phishing Attack in comparison to the 1 – 250 and 501 – 1000 ranges respectively); In terms of industry, the Retail sector is almost twice as likely to be the victim of a Phishing Attack in comparison to other sectors, While in terms of employees, staff in the areas of HR, Payroll and Finance are targeted in 96% of advanced Phishing Attacks.

Like all business operations, Cyber Security relies on People, Processes and Products/Technologies, i.e. The three P's. Traditionally, organisations have relied exclusively on Processes and Technology for Cyber Security purposes, despite the fact 95% of all Cyber Attacks are the result of human error e.g. Clicking on malicious URLs in e-mails, Opening malicious e-mail attachments, Disclosure of credentials, etc.

This overreliance on technology is severely flawed as Cyber Security technologies are not 100% effective – a fact that the manufacturers of such software readily admit (Wall Street Journal, 2014). As mentioned previously, Spam/Phishing filtering software has a success rate of 93%, while Anti-Virus and Anti-Malware technologies only respond to previously known Cyber Attacks – and as of 2016 - it has never been easier to develop or acquire custom built malware that circumvents such software.

When technical solutions fail or underperform, people are the last line of defence. Independent research has shown that targeting the People element of The Three P's in Cyber Security - via Cyber Security Awareness Training (including simulated Phishing Attacks) – can drastically reduce the likelihood of a successful Cyber Attack via Phishing (the number #1 form of Cyber Attack). **By decreasing the Read, Click/Download and Disclose rate of Phishing E-mails from the industry average of 30%/12%/12% to 3%/1%/1%, organisations can achieve a risk likelihood reduction of 99.93%.**

1. 50 Employees: $19,750 USD;
   250 Employees: $98,750 USD;
   500 Employees: $197,500 USD;
   1000 Employees: $395,000 USD;
   2500 Employees: $987,500 USD.
   5000 Employees: $1,975,000 USD.

Cyber Security: 2017

*"Cyber Security Is Not Just the Responsibility of the I.T. Department, It's **Everyone's** Responsibility."*

In recent years, coverage of Cyber Security incidents in the mainstream media has increased dramatically to the point that it is now common for some form of incident to be reported on a daily basis. While the world has no doubt become more aware of Cyber Security as a result of such reporting, the fact remains that Cyber Criminals are using increasingly more complex and sophisticated mechanisms as part of their day-to-day activities.

While technologies such as Anti-Virus, Anti-Malware and Firewall's play an essential role in securing modern-day digital devices and networks, they are by no means perfect. Such technologies only provide coverage against those Cyber Attacks which are already known to Anti-Virus and Anti-Malware software vendors (AV Comparatives, 2017; Wall Street Journal, 2014). With the advent of Executable Compression, Code Obfuscation and Polymorphic/Metamorphic Malware, Cyber Criminals now have the ability to easily produce Malware that avoids detection by market leading Anti-Virus and Anti-Malware software. As a result of this, Cyber Criminals are now in a position whereby they can use custom-built Malware for each individual attack that they carry out (therefore drastically increasing the likelihood of a successful attack) (Help Net Security, 2016).

> *"At The Core Of All Modern Business Operations Are Three Key Elements: People, Processes and Technology. In The Case Of Cyber Security, **People** Have Always Been The Weak Link."*

At Cyber Risk Aware, we do not focus on the development of technical solutions that defend against these attacks. Instead, we focus on providing cyber security awareness training with a view to reducing cyber risks for business and staff (both at home and in the workplace). Our Research has shown that Human Error has been identified as the Primary or Secondary Root Cause in 95% of all Cyber Security Incidents (IBM, 2014). While other companies focus on technical solutions, we help create a "Human Firewall" – intelligent cyber security aware employees that help protect organisations against the threat posed by Cyber Criminals. As Cyber Criminals change their tactics and approaches, it is important that companies – and their employees – stay up to date with the latest and upcoming Cyber Security threats and how to prevent them.

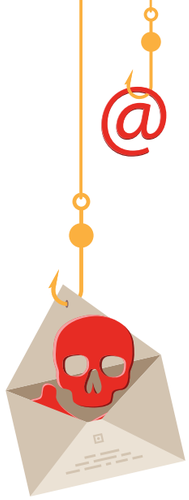
Phishing

"Phishing Is Much More Effective Than You Might Think. Numerous Studies Have Shown That Approximately 30% of All Phishing E-Mails Get Opened; 12% of Attachments or Links Get Clicked/Downloaded (1 In Every 8 People) and a Further 12% Proceed To Disclose the Information Requested In the Phishing E-Mail. To Those Who Are Conscious of Cyber Security, These Figure May Seem Quite High; However Cyber Criminals Have Known This for Years – It's Why Phishing Remains the #1 Form Of Cyber Attack (Verizon, 2017).

Anyone with access to an e-mail account has no doubt received a phishing e-mail. Classic examples include receiving unsolicited e-mails from what appears to be a Bank, Social Media Company or E-Commerce company requesting that you reset your user account password or PIN number. The concept behind such e-mails is to trick the recipient into believing that the e-mail was sent from a legitimate entity in the hope that the recipient will carry out the action stated in the e-mail, e.g. password reset (thereby disclosing their current password in the process). Such e-mails often contain links to malicious websites masquerading as legitimate entities in the hope that recipients will disclose the information requested in the phishing e-mail. To the untrained eye, such e-mails and websites may appear perfectly legitimate.

In the event of a phishing attack succeeding, i.e. the requested credentials have been disclosed; Cyber Criminals act quickly: Over 70% of all money stolen in phishing attacks is stolen within six hours of credential disclosure, with the remaining 30% being extracted over the following 18 hours (with little or no activity taking place after 24 hours) (ISACA, 2017).

From a technical perspective, it may seem like a trivial process for e-mail providers and spam filters to identify phishing e-mails due to the fact that such e-mails are typically sent out in huge quantities to a vast number of recipients; however the fact remains that only 93% of Phishing e-mails are detected – the remaining 7% end up in the Inbox with other legitimate e-mails – and that's where the danger lies (ISACA, 2017).



On average, 1 in every 1,846 e-mails sent globally is a Phishing e-mail; however certain business sectors and company sizes are targeted more often than others (see Table 1 and Table 2) (Ponemon Institute, 2016)

INDUSTRY	PHISHING EMAIL RATIO
Retail	1 In 690
Public Administration	1 In 1198
Agriculture, Forestry & Fishing	1 In 1229
Services	1 In 1717
Manufacturing	1 In 1999
Finances, Insurance & Real Estate	1 In 2200
Mining	1 In 2225
Wholesale Trade	1 In 2226
Construction	1 In 2349
Transportation & Public Utilities	1 In 2948
Energy	1 In 2349
Healthcare	1 In 2711

Table 1: Phishing Ratio by Sector (Ponemon Institute, 2016).

COMPANY SIZE	PHISHING EMAIL RATIO
1 - 250	1 In 1548
251 – 500	1 In 758
501 – 1000	1 In 1734
1001 – 1500	1 In 2212
1501 – 2500	1 In 1601
2501+	1 In 2862

Table 2: Phishing Ratio by Company Size (Ponemon Institute, 2016).

Cyber Risk Aware
Creating your human firewall!

Spear Phishing

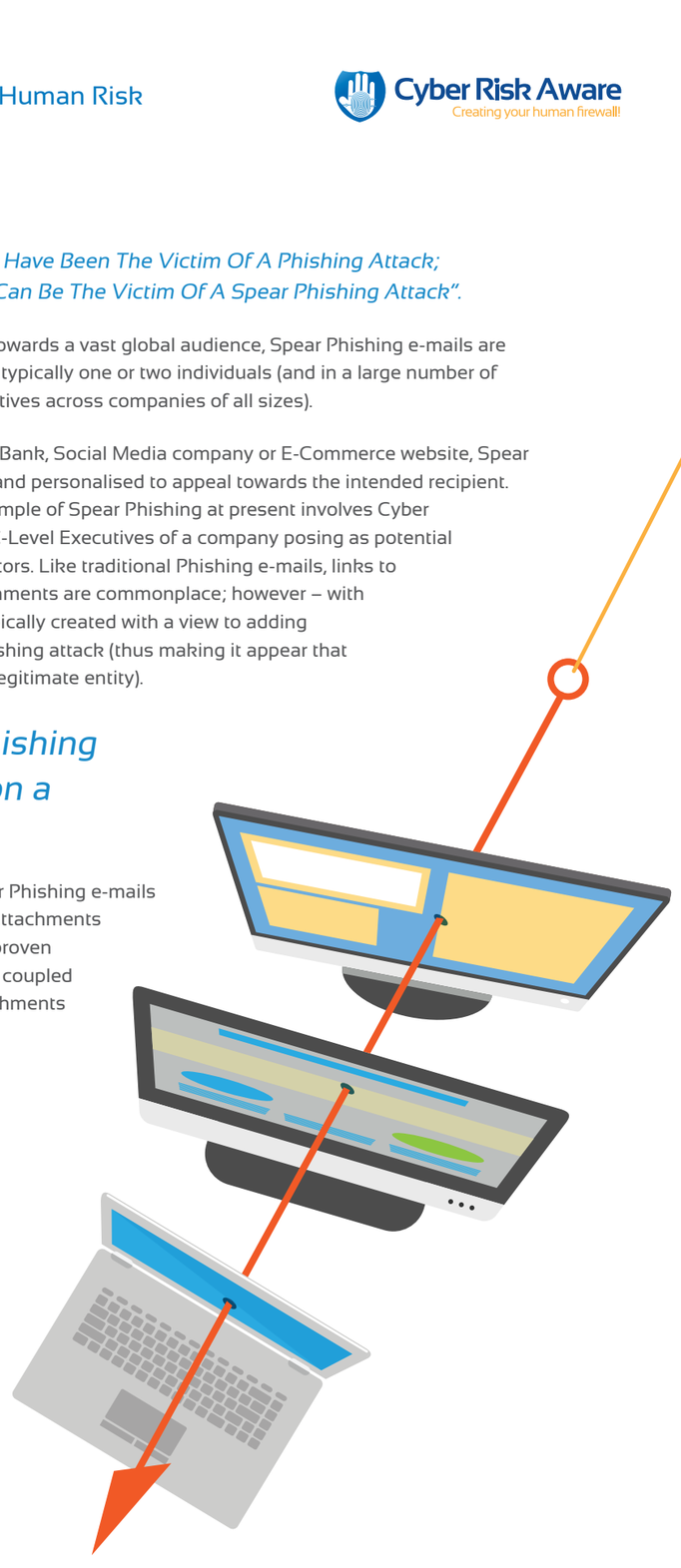
*"You May Never Have Been The Victim Of A Phishing Attack; However **Anyone** Can Be The Victim Of A Spear Phishing Attack".*

While Phishing e-mails are marketed towards a vast global audience, Spear Phishing e-mails are marketed towards very small groups – typically one or two individuals (and in a large number of modern cases – various C-Level Executives across companies of all sizes).

Rather than appearing to come from a Bank, Social Media company or E-Commerce website, Spear Phishing e-mails are specially crafted and personalised to appeal towards the intended recipient. A simple and particularly common example of Spear Phishing at present involves Cyber Criminals e-mailing the CEO or other C-Level Executives of a company posing as potential or existing customers/suppliers/investors. Like traditional Phishing e-mails, links to external websites and malicious attachments are commonplace; however – with Spear Phishing - such websites are typically created with a view to adding a layer of authenticity to the Spear Phishing attack (thus making it appear that e-mails have originated from within a legitimate entity).

"In Essence, Spear Phishing Is a Targeted Attack on a Chosen Individual".

Like traditional Phishing e-mails, Spear Phishing e-mails are also accompanied with malicious attachments and the use of such attachments has proven extremely potent in recent times when coupled with Custom Built Malware (such attachments typically masquerade as Brochures, Catalogues, Invoices, etc.).



Cyber Risk Aware
Creating your human firewall!

Whitepaper | Cyber Risk is a Human Risk

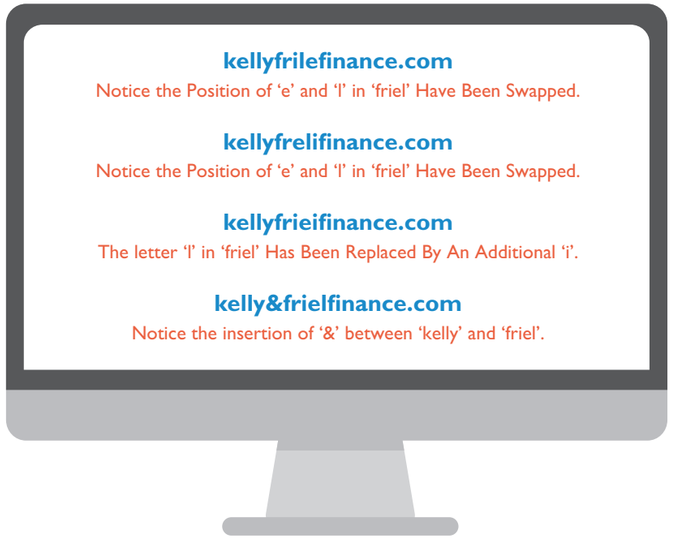
CEO Fraud

"The Amount Of Publically Available Information About Companies and Individuals Makes CEO Fraud Trivially Simple: Company Websites, Social Media Profiles, Advertisements, Company Registration Listings, Financial/Tax Records And Media Coverage – All The Information You Need To Know To Get Started Is Available At The Click Of A Mouse. In Addition, The Poor Regulation Surrounding The Sale And Purchase Of Internet Domain Names – Particularly Dot Com Domain Names (.com) - Means That Anyone Can Purchase Domain Names For Use In CEO Fraud Attacks."

In addition to Phishing and Spear Phishing, Cyber Criminals have also adopted another highly effective e-mail based attack in recent years: CEO Fraud.

While Phishing and Spear Phishing attacks attempt to trick the recipient into clicking links, downloading malicious attachments or disclosing valuable information, CEO Fraud attempts to trick e-mail recipients into believing that e-mails have been sent to them by company management or other superiors in the work place (when in fact, such e-mails have been sent by Cyber Criminals). CEO Fraud e-mails often contain requests for the targeted employees to carry out tasks on behalf of the 'e-mail sender' (as the name of the attack suggests, the most commonly impersonated 'email sender' in CEO Fraud e-mails are C-Level Executives). Such requests often include the transfer of funds to a bank account or the forwarding of confidential/private information via e-mail. An estimated 80% of CEO Fraud e-mails request such actions to be carried out in their opening e-mails; however the remaining 20% of attacks are much more sophisticated in that the 'sender' holds a conversation with the targeted employee (via e-mail) before then requesting that an action be carried out (thus reducing suspicion). In terms of CEO Fraud targets, employees working in HR, Finance and Payroll are targeted in 96% of instances (Proof Point).

As part of CEO Fraud attacks, Cyber criminals typically purchase domain names similar to that of their target and then proceed to create e-mail accounts with usernames which replicate those of the target organisation. Such domain names are often subtle – difficult to spot - variations on the targets legitimate domain name. As an example of this, consider a company named **'Kelly and Friel Finance'** with legitimate domain name kellyfrielfinance.com. When attempting a CEO Fraud attack against this company, Cyber Criminals may purchase and utilise one or more of the following domain names in order to carry out their attack:



Ransomware: A Game Changer for Cyber Criminals.

"In The Past, Malware And Spyware Was Largely Used To Monitor Users Activities And Steal Information Such As Credit Card Numbers. With Ransomware, Cyber Criminals No Longer Need To Steal Information - They Lock Access To Victims Data And Then Force The Victim Into Paying A Substantial Ransom In Order To Regain Access To Their Data."

Pre-2012, Cyber Criminals largely focussed on stealing information such as credit card details or passwords for financial gain; however, 2012 saw a drastic change in tactics. It is now common practice for Cyber Criminals to hold computer users to ransom by locking access to their system and/or data and requesting that victims pay a ransom in order to regain access. Such software is commonly referred to as Ransomware and it is particularly relevant at present given the significant media coverage afforded to the WannaCry Ransomware which affected a large number of leading global organisations in May 2017 (including the NHS, Telefonica and FedEx) (Symantec, 2017) and the Petya Ransomware in June 2017 (The Telegraph, 2017).

Ransomware typically works by generating highly randomised passwords (often thousands of characters in length) which are then used to encrypt victims' data. Having generated the password and encrypted all data, the Ransomware software then transmits a copy of this password back to the Cyber Criminals command centre where a copy of the password is retained until the victim has paid the requested ransom. Upon payment, the Cyber Criminals will either provide the user with this password or decrypt their data for them. Unfortunately, due to the length and highly randomised nature of these passwords, victims are not in position to decrypt their data without payment of the ransom (note that cases do exist whereby ransoms have been paid but the associated data has not been decrypted).

From a financial perspective, Ransomware has proven to be an extremely lucrative industry for Cyber Criminals and is now frequently used in conjunction with Phishing e-mails (with research showing that 93% of all Phishing e-mails now contain Ransomware as an attachment (Verizon, 2017)). The CryptoLocker Ransomware active in 2013 resulted in an estimated $3 million gain for the perpetrators (at a cost of $300 per victim (ZD Net, 2013)), while the CryptoWall Ransomware active in 2015 is estimated to have resulted in an estimated $18 million gain for the perpetrators (FBI, 2015).

Recalling his experience of dealing with a Ransomware attack in 2013, Shaun Mc Brearty – an Assistant Lecturer in Computing at I.T. Sligo in the Republic of Ireland - had the following to say:

"In 2013, I was working for a UK manufacturing company in the SME sector that fell victim to the CryptoLocker Ransomware (one of the first major worldwide incidents involving Ransomware). The attack took out all the companies' major operational data – including CNC instruction – and brought the company to a complete standstill – no manufacturing, no sales: nothing. The Ransomware demanded £2,000 GBP to decrypt the data, but thankfully we didn't have to pay it as all data was backed up to an external server which we were able to restore; however the company lost over 25 hours of manufacturing time as a result of the attack. When I investigated the incident, I managed to track the source of the Ransomware to the PC of a recently hired trainee Accountant (it was his second day on the job). The Ransomware actually entered the companies' network via a spear phishing e-mail addressed to him from what appeared to be one of our suppliers. The Ransomware was embedded within an attached PDF invoice so it was a very easy mistake to make. Aside from the lost manufacturing time, the knock-on effects of the attack were actually very serious for the company. The attack caused us to miss the deadline for our very first order for a new customer (a major UK retailer who we had spent almost six months negotiating a partnership with). While I can't recall the exact figures, I know that the company was penalised financially for missing this deadline. And to make matters worse, another member of staff was targeted with Ransomware e-mails later in the week causing us to lose another full day's manufacturing."

Malware as a Service (MAAS) and Phishing as a Service (PhAAS): The Commercialisation of Cyber Crime

"Do Not Underestimate the Threat Posed By Malware as a Service (MAAS) or How Easy It Is To Access And Use These Services. Any Basic Dark Net/Deep Web Search Engine and even Public Internet Chat Forums - Such As Reddit - Can Point You In The Direction Of Cyber Criminals And Malware For Hire Within A Matter Of Seconds – It's That Simple."

2016 and 2017 saw a dramatic shift in the business model of Cyber Crime. Previously, it was commonplace for Cyber Criminals to develop their own Malware and carry out their own attacks; however recent times has seen Cyber Criminals make their Malware available for use by other potential Cyber Criminals for a fee, a la Software As A Service (SAAS). In some cases, Cyber Criminals are selling individual pieces of Malware on Dark Net Marketplaces at a set cost; while others are offering subscription-style services whereby subscribers have access to all new and updated Malware developed for the duration of their subscription. In an article posted in June 2017, the Infosec Institute reported that Cyber Criminals were offering the use of modified versions of the CryptoLocker Ransomware (discussed in the previous section) for a fee of USD $100 on the Dark Net (as mentioned previously, CryptoLocker extorted approximately USD $3 million from its victims in 2013 and 2014) (InfoSec Institute, 2017).

In relation to Phishing as a Service (PhAAS), Cyber Criminals are now offering customer's access to the vast array of E-Mail Servers that they control and have access to. Previously, Cyber Criminals had to build up their own network of E-Mail Servers in order to utilise Phishing on a large scale; however with PhASS they have a pre-existing network available to them at a low cost. In some cases Cyber Criminals are now providing Data Analytics and Business Intelligence Reports as part of their PhAAS solutions with a view to providing their customers with in-depth, granular information on the success of their Phishing campaigns (such solution are on par with, if not better than a number of the leading legitimate e-mail marketing solutions). Such data can include: Number of e-mails opened (including the e-mail address of those recipients who opened the e-mail so that they can be targeted further), Number of e-mails where attachments were downloaded, number of e-mails where embedded URLs were clicked as well as identifying specific Countries/Regions/Cities (and even individuals) where attacks are proving to be more successful than others (Imperva, 2016).

In essence, Malware as a Service and Phishing as a Service have made the business of Cyber Crime easily accessible to those who did not possess the necessary technical skills to do so previously - which may go some way towards explaining the dramatic increase in Cyber Crime during 2016 and 2017. In order to provide such services, Cyber Criminals now operate in a manner that is comparable to legitimate software development companies with people employed in roles such as Malware Development, Malware Testing (to ensure that developed Malware is not detected by leading Anti-Virus, Anti-Malware, IDS and Firewall systems), Instruction Manual Authors (to provide How-To Guides for Malware users) and Phone Based/E-Mail Based Customer Support.

Am I At Risk?

"The Perception: 'It'll Never Happen to Me or My Company'; The Reality: 'Every Person with Access to an E-mail Account In Your Organisation Is a Potential Risk – And It Only Takes One Mistake For That Risk To Become A Reality'.

Large organisations, SMEs and the average home PC user are all at risk from Cyber Crime –particularly from Phishing, Spear Phishing, CEO Fraud, Purpose Built Malware and Ransomware. Anti-Virus and Anti-Malware software vendors are very much a step behind Cyber Criminals in these areas at present as they struggle to develop reliable defensive technical solutions. Cyber Criminals are aware of this and have dramatically increased their output in 2016 and 2017 while this gap remains open.

In terms of Ransomware, there were an estimated 638 million Ransomware attacks in 2016 alone (One for every Twelve people on the planet) – up from 3.8 million in 2015 (a 167 fold increase) – with industry experts forecasting even further growth into 2017 and beyond.

In terms of Phishing, the automated detection rate of e-mail providers clearly needs to improve. While 93% is an impressive detection ratio, the sheer quantity of phishing e-mails circulating globally ensures that a significant number of e-mails fall into the remaining 7% which end up in the Inbox. Phishing is very much a game of number and the Cyber Criminals will persist until their Phishing campaigns fall within this category.

In relation to Spear Phishing, its very nature makes it neigh on impossible to develop a reliable defensive technical solution as such e-mails appear to be no different to genuine e-mails on the surface. As such Cyber Criminals will continue to exploit this approach. A careful, cautious and analytical approach is required by the recipient; a process covered by Cyber Risk Aware in our comprehensive online training program.

In addition to providing training solutions, Cyber Risk Aware also provides customers with access to a Mock Phishing platform whereby they can test and monitor employee behaviour when handling Phishing e-mails. In our first year of operation, our results show that an average of Four in Ten employees read the contents of general Phishing e-mails received in their corporate inbox (with Seven in Ten reading CEO Fraud style Phishing e-mails) while an astonishing One in Eight employees clicked on links to external websites included in such e-mails and/or opened attachments.

When technical solutions fail, people are the last line of defence, and as mentioned previously, it only takes a mistake from one employee for a Ransomware or Malware attack to become a reality; don't get caught out.

From a financial perspective, a study by ISACA has shown that the cost incurred by companies as a result of Cyber Attacks is directly proportionate to the number of employees in an organisation (ISACA, 2017) – with the Ponemon Institute calculating the average cost of an individual Cyber Attack per employee at USD $394.56 (see Table 3).

Average cost of cyber attack by company size				
1 – 250	251 – 500	501 - 1000	1001 – 2500	2501 - 5000
$395-$98,640	$99,035 - $197,280	$197,675–$394,560	$394,955–$986,400	$986,795-$1,972,800

Table 3: Average Cost of Cyber Attacks by Company Size.

2. Slightly above the independent research estimate of Three in Ten.
3. This figure incorporates loss of money as a result of Phishing and Ransomware, cost of repairing equipment damaged in a cyber-attack and loss of productivity - other factors such as damaged business reputation are difficult to quantify (Ponemon Institute, 2016).

How Can I Reduce My Risk?

At Cyber Risk Aware, we provide cyber security awareness training with a view to reducing cyber risks for businesses and their staff. Independent Research has shown that Human Error has been identified as the Primary or Secondary Root Cause in 95% of all Cyber Security Incidents (IBM, 2014); as such, we help create the "Human Firewall" – intelligent cyber security aware employees that help protect organisations against the threat posed by Cyber Criminals.

Our comprehensive online training platform has been used by Fortune 500 companies, FTSE 100 companies and is currently in use at a number of Cyber Insurance companies worldwide to determine and lower customer risk (and premiums).

For companies with 100 employees or less we offer a bundle of 20 users at a cost of £/€/$400.00 and 50 users at a cost of £/€/$700.00. For companies with 101 or more employees, prices are charged on a per user basis with prices decreasing for larger quantities of user (see Table 4).

For more information, see **http://www.cyberriskaware.com.**

User Volume Pricing Guide (101+ Users)			
101 – 500	501 - 1000	1001 - 2500	2501 - 5000
£/€/$11.00	£/€/$9.00	£/€/$7.00	£/€/$5.00

Table 4: User Volume Pricing Guide.

Our training program aims to reduce the Read Rate of phishing e-mails from 30% within organisations to 3%, the Click/Download Rate from 12% to 1% and the credential Disclosure Rate from 12% to 1%. Achieving this level of compliance results in an overall reduction in Cyber Security risk by 99.93% - see Table 5 for the associated financial impact both with and without Cyber Security Awareness Training.

Financial Risk Before And After Training.)				
1 – 250	251 - 500	501 - 1000	1001 – 2500	2501 - 5000
$395-$98,640	$99,035 - $197,280	$197,675–$394,560	$394,955–$986,400	$986,795-$1,972,800
$0.27 - $68	$69 - $135	$135 – $270	$270 - $675	$675 – $1350

Table 5: Financial Risk Before and After Training..

Testimonials

Vincent Nolan - Applegreen

Applegreen Plc utilised the Cyber Risk Aware solution to quickly assess and demonstrate to the business owners the risks associated with the increasing prevalence of Phishing emails and the importance of providing staff with effective Security Awareness Training.

The deployment was very quick and our IT department were extremely impressed with the fact it was non-intrusive and simple to deploy. The ability to generate personalised phishing emails was simple and very effective.

I can highly recommend the service.

Séamus Hogan - Smyths Toys

The human firewall is the hardest firewall to manage and maintain but the most important. Security awareness never stops and using Cyber Risk Aware allows us to continually educate, test and train all our users. Whenever the latest scam goes viral we are immediately able to simulate this attack and raise staff awareness without compromising our network or users.

Our IT Security Team have seen a significant reduction in requests from employees checking if an email is something legitimate or Spam/fraud as they are now more aware. Cyber Risk Aware is a huge factor in delivering this education and awareness to the end user.

Works Cited

AV Comparatives. (2017, June 12). Retrieved July 5, 2017, from www.av-comparatives.org: https://www.av-comparatives.org/wp-content/uploads/2017/06/avc_factsheet2017_05.pdf

FBI. (2015, 6 23). CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES. Retrieved 7 5, 2017, from IC3: https://www.ic3.gov/media/2015/150623.aspx

Help Net Security. (2016, 2 29). The Rise Of Polymorphic Malware. Retrieved 7 5, 2017, from Help Net Security: https://www.helpnetsecurity.com/2016/02/29/the-rise-of-polymorphic-malware/

IBM. (2014, 9 2). The Role of Human Error in Successful Security Attacks. Retrieved 7 5, 2017, from Security Intelliegnce: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

Imperva. (2016). Phishing Made Easy: Time To Rethink Your Prevention Strategy? Retrieved 7 5, 2017, from Imperva: https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

InfoSec Institute. (2017, 6 5). Malware-As-A-Service. Retrieved 7 5, 2017, from InfoSec Institute: http://resources.infosecinstitute.com/malware-as-a-service/

ISACA. (2017). ISACA Digital Journal. Retrieved 2017, from Phishing Detection And Loss Computation Model: http://www.isacajournal-digital.org/isacajournal/2017_volume_1?pg=24#pg24

Ponemon Institute. (2016, 10). Retrieved 7 5, 2017, from University of Arkansas: http://ualr.edu/itservices/files/2016/10/Ponemon_Institute_Cost_of_Phishing.pdf

Proof Point. (n.d.). BEC Survival Guide: Managing Business Email Compromise and Impostor Threats. Retrieved 7 5, 2017, from Proof Point: https://www.proofpoint.com/us/resources/white-papers/bec-survival-guide

Symantec. (2017, 5 12). What You Need To Know About The WannaCry Ransomware. Retrieved 7 5, 2017, from Symantec: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

The Telegraph. (2017, 6 27). Petya Cyber Attack: Ransomware Spreads Across Europe With Firms In Ukraine, Britain And Spain Shut Down. Retrieved 7 5, 2017, from The Telegraph: http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

Verizon. (2017, 7 5). Verizon Enterprises. Retrieved 4 3, 2016, from Verizon 2016 Data Breach Investigations Report: www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Wall Street Journal. (2014, 5 4). Symantec Develops New Attack on Cyberhacking. Retrieved 7 12, 2017, from Wall Street Journal: https://www.wsj.com/news/article_email/SB10001424052702303417104579542140235850578-lMyQjAxMTA0MDAwNTEwNDUyWj

ZD Net. (2013, 12 23). CryptoLocker's Crimewave: A Trail Of Millions In Laundered Bitcoin. Retrieved 7 5, 2017, from ZD Net: http://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/