HERBERT
SMITH
FREEHILLS

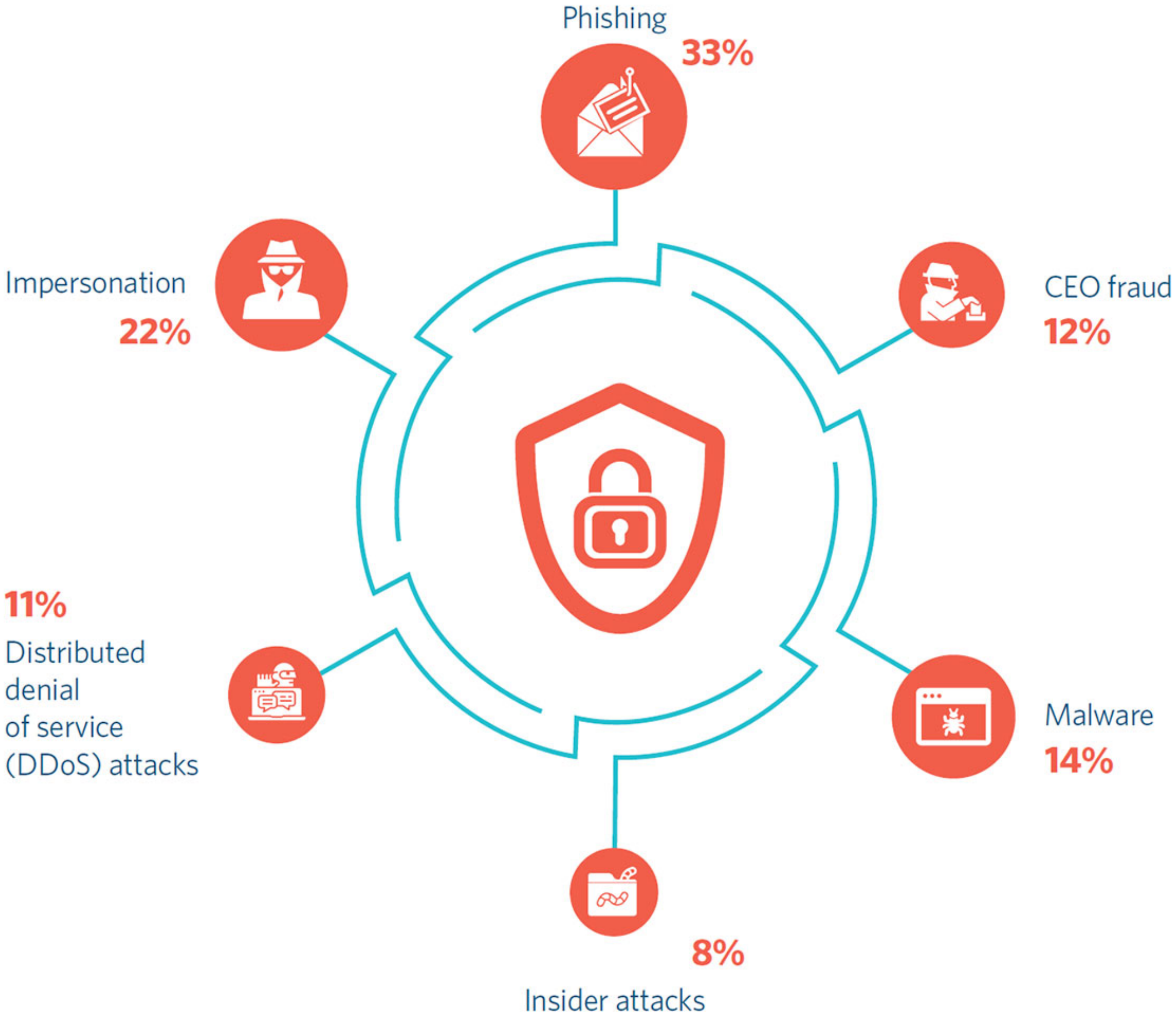
CYBER SECURITY IN FOCUS

26 May 2020 | London

Our survey shows that trust companies consider cyber attack to be one of the greatest challenges they face.

The results show that trustees consider phishing, impersonation and malware to be the main cyber security risks they face. Some 33% of respondents said they saw phishing as the main risk whilst 22% identified impersonation as a main risk and 14%, malware.

WHAT ARE THE MAIN CYBER SECURITY RISKS FACED BY TRUSTEES?



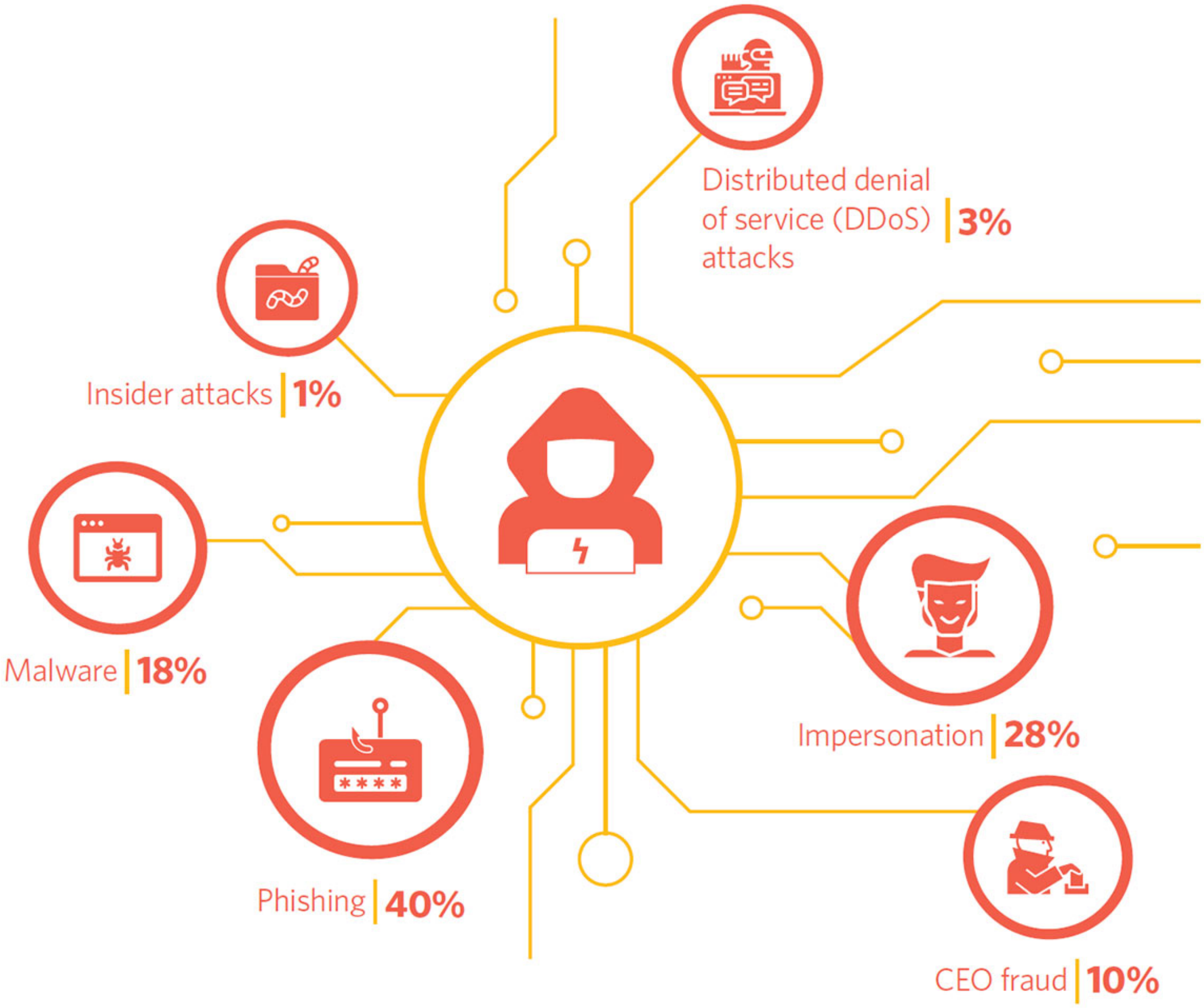
This is perhaps unsurprising as many cyber attacks – even highly sophisticated nation-state attacks – need an initial entry point and this is commonly one or more of these three. The scale of this problem is enormous - the National Cyber Security Centre, for example, estimates that 1.5 million new phishing sites are created around the world every month.

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, password and credit card details by masquerading as a trustworthy entity in email, text or social media. Phishing attacks can install malware (software which is specifically designed to disrupt, damage or gain unauthorised access to a computer system), with a view to infiltrating systems or stealing intellectual property or money.

Impersonation, sometimes in conjunction with phishing or spear phishing attempts, involves the hacker pretending to be someone trusted (the friendly IT support person, a customer services representative from a bank and so on) with a view to tricking the victim into voluntarily doing something. In the trust company world in particular, impersonation might come in the form of emails purporting to be from beneficiaries asking for distributions from the trust fund. Paul Hodgson of Butterfield Trust in Guernsey mentioned their experience that the small number of phishing attempts that their business sees result from successful attacks on beneficiaries and settlors which are then used to create sophisticated template emails which require a combination of a high level of training to ensure that relationship managers identify them, call backs to known contact numbers to combat them and a dedicated Cyber Security team that detect and respond to attacks.

Perception of the main risks was born out by reality. Some 40% of the trust companies surveyed said they had suffered a phishing attack and 28% an impersonation attack. Some 18% had experienced a malware attack. CEO fraud and distributed denial of service were far rarer with only 10% and 3% of trust companies experiencing attacks of this kind. Only 1% had suffered an insider attack, which is perhaps indicative of rigorous screening of personnel both prior to and during employment.

WHICH OF THE FOLLOWING TYPES OF CYBER-ATTACKS HAVE YOU SUFFERED?



Bob Rodger, the Head of Information Security at Butterfield Trust commented that ensuring high standards of cybersecurity is a business imperative - they regard the ability to deliver fiduciary services in a secure way as a critical component of their relationships with settlors, beneficiaries and the range of third parties.

So, how can trust companies defend themselves? Training people to spot attacks of this kind is an important part of defence and 44% of respondents said that they were doing this.

However, there are many other “hard basics” that can be deployed using a layered approach to bolster your security defences further.

One layer might involve making it harder for attackers to reach users. This might involve filtering or blocking incoming emails, implementing anti-spoofing controls and reducing the amount of information you make public on websites or social media. For example, hackers can often discern a significant amount of information about the systems, software and data centres used by a business, simply by looking at the LinkedIn profiles of their IT support staff.

There are also steps you can take to protect your organisation from the effects of undetected phishing emails. You might use two factor authentication, which makes it harder for attackers to access accounts, ensure that authorisation gives privileges only to people who need them and install endpoint monitoring and protection software to try to intercept or detect malware. You can also help protect your users from malicious actors by use of a proxy server – a server which screens incoming and outgoing web communications – and ensuring that browsers and other software are up to date.

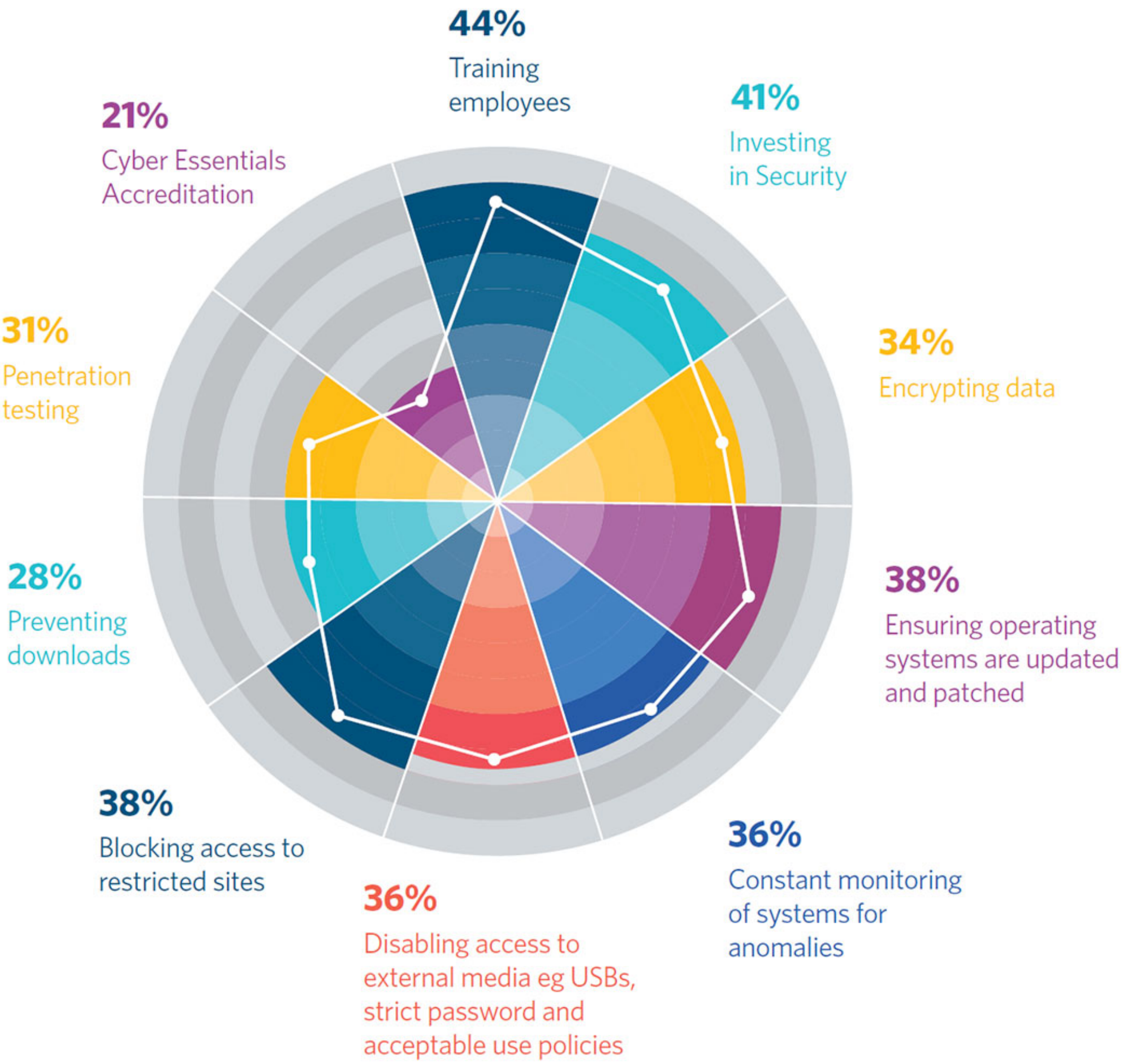
Much of this was borne out by the survey results. Some 41% of respondents said they were investing in security, with 38% saying that they ensured operating systems are updated and patched, 38% saying they blocked access to restricted sites, 36% saying they disabled access to external media and 28% saying they prevented downloads.

Trust companies were active in threat detection, with 36% saying they constantly monitored systems and 31% carrying out penetration testing to identify vulnerabilities and see whether their defences could withstand attack.

Only a third of trust companies (34%) said they chose to encrypt data, which may reflect the challenges of implementing some types of encryption (such as on-disk encryption) without interrupting business as usual.

These types of measures are also contemplated by various accreditations such as Cyber Essentials and Cyber Essentials Plus. A fifth of those surveyed were adopting Cyber Essentials accreditation, a government-backed scheme to ensure a minimum level of cyber resilience.

WHAT ARE YOU DOING TO TACKLE THE CYBER SECURITY RISKS FACED BY TRUSTEES?



***respondents were able to choose more than one option**

Regulators expect organisations to prevent attacks and it is prudent to obtain legal advice regularly upon the regulators' expectations and how they are developing in line with rapidly evolving technology. The GDPR reflects that the security one implements should take into account "the state of the art". Seven of the ten top fines by data protection regulators in Europe last year were for inadequate technical and organisational measures under the security of processing provisions of Article 32 of the GDPR. The Information Commissioner's Office in the UK has recently powerfully emphasised the importance of "hard basics". It has recently issued two fines following personal data breaches at the top level allowed under the pre-GDPR regime - £500,000 - for inadequate technical and organisational measures. In one case, the ICO specifically mentioned failure to attend to network segregation, firewalls, software patching, regular vulnerability scanning, penetration and vulnerability testing, application whitelisting, systems for logging and monitoring, updating software, point to point encryption, secure domain administrator accounts and adopting standard builds for all system components. In the other, it noted that the entity had failed to satisfy four out of five of the National Cyber Security Centre's basic Cyber Essentials guidance.

KEY TAKEAWAYS

Given that even the most secure organisations can still suffer successful attacks, there is an increased emphasis on organisations' ability to respond to, recover and learn from attacks quickly. Financial Services regulators are asking firms to ensure that they can deliver operational resilience in their important business services. Accordingly, rapid detection and containment of any cyber incident is essential and any measures to protect your organisation should include a way to deliver prompt and effective incident response, which can do much to mitigate the harm any attack might cause and may reduce the likelihood of regulators taking enforcement action against you.

Listen to our accompanying podcast below

Herbert Smith Freehills Podcasts · Private Wealth & Charities Podcast EP10: Trust Companies Survey – Cyber security

---

To review the other articles in this series, please click on the link below

Herbert Smith Freehills Trust Companies Survey: Navigating Troubled Waters

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

KATE MACMILLAN
CONSULTANT, LONDON
+44 20 7466 3737
kate.macmillan@hsf.com

RICHARD NORRIDGE
PARTNER, HEAD OF PRIVATE WEALTH AND CHARITIES, LONDON
+44 20 7466 2686
richard.norridge@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.