HERBERT SMITH FREEHILLS

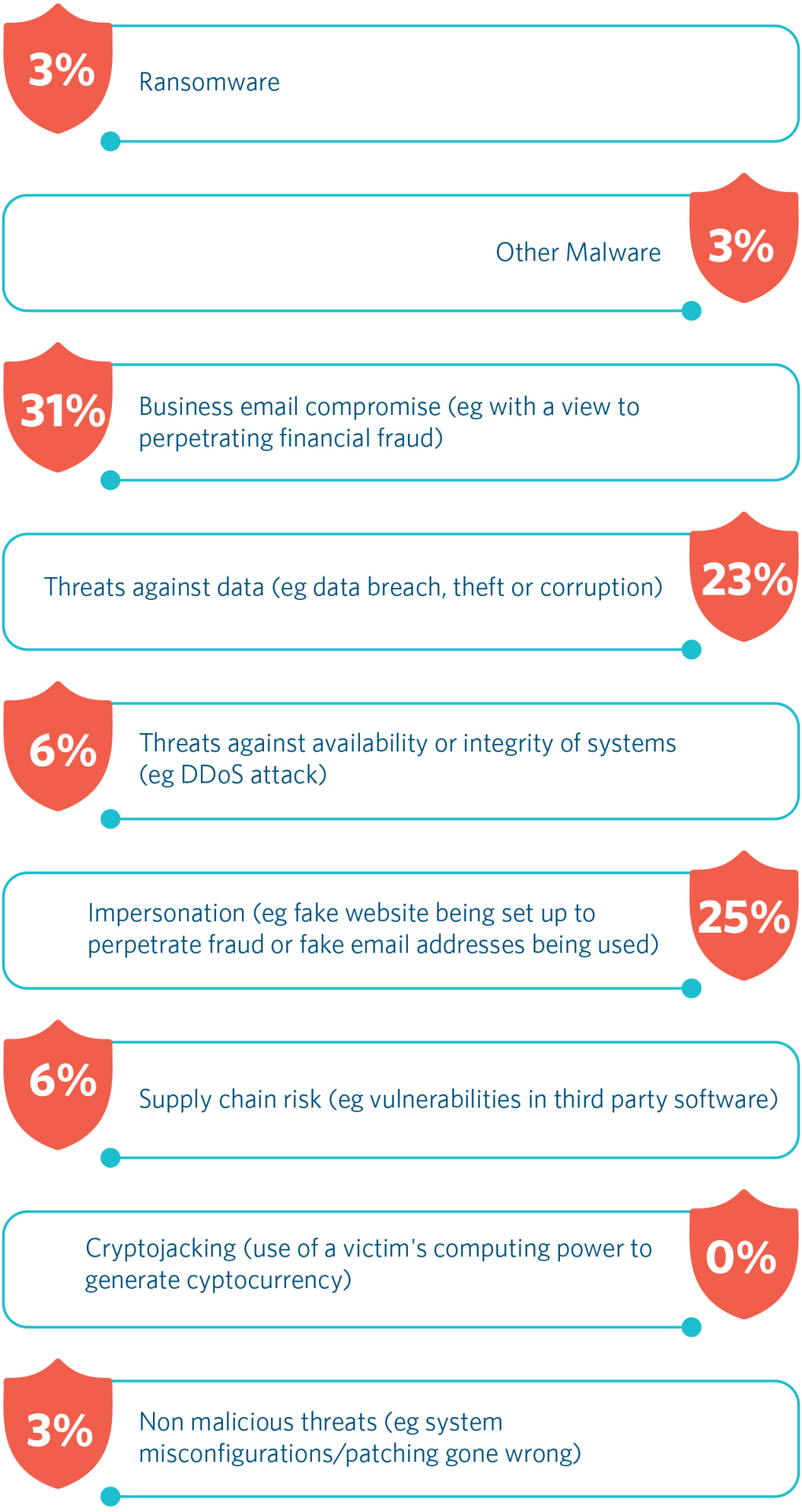
TRUST COMPANIES SEE CYBER SECURITY AS KEY BUSINESS RISK

29 June 2022 | London
Legal Briefings

Our survey confirms that trust companies continue to see cyber security as a key business risk. This is in line with companies in other areas: in IBM's 25th edition of "The CEO Study", drawn from interviews with 3,000 CEOs worldwide, CEOs ranked cyber risk as their greatest organisational challenge (coming just behind sustainability and regulation).[1] Further the Proofpoint 2022 Voice of the CISO[2] Report[3] – which surveyed 1,400 CISOs from around the world between February and March 2022 - states that some 48% of surveyed CISOs considered their organisation was at risk of suffering a material cyber-attack in the next 12 months, with one third rating the risk as very high. The Report also showed that CISOs considered large organisations were more acutely aware of the risk.[4]

Our survey also shows that trust companies see Business Email Compromise ("BEC") as the main category of risk – with 31% seeing BEC as the main risk and some 15% of trust companies having suffered a BEC attack in the last year.

WHAT IS THE MAIN CYBER AND DATA SECURITY RISK FACED BY YOU AS A TRUSTEE IN THE 12 MONTHS?


3%
Ransomware
Other Malware
3%
31%
Business email compromise (eg with a view to perpetrating financial fraud)
Threats against data (eg data breach, theft or corruption)
23%
6%
Threats against availability or integrity of systems (eg DDoS attack)
Impersonation (eg fake website being set up to perpetrate fraud or fake email addresses being used)
25%
6%
Supply chain risk (eg vulnerabilities in third party software)
Cryptojacking (use of a victim's computing power to generate cyptocurrency)
0%
3%
Non malicious threats (eg system misconfigurations/patching gone wrong)

The fact that BEC is in pole position is not surprising given that BEC is the cyber threat which accounts for the largest financial losses globally. For example, the FBI's Internet Crime Report for 2021 estimated that BEC scams cost US business nearly $2.4 billion in 2021.[5]

There are various definitions of BEC fraud. Perhaps the most useful one is the National Cyber Security Centre's, which defines it as "a form of phishing attack where a criminal attempts to trick a senior executive – or budget holder - into transferring funds, or revealing sensitive information."

There are a number of techniques we see criminals use often in BEC attacks.

One simple method criminals use is to set up an email address that looks like a legitimate email address – billgates@mlcrosoft.com instead of bill.gates@microsoft.com, for example, to make a person think they are corresponding with someone legitimate rather than a fraudster. Watch out for replacement characters (so-called homoglyphs, which in some cases are indistinguishable from the legitimate character), obscure or unexpected top-level domains or suspicious sub-domains in email addresses (eg Bill.Issuer@e*xternalsupplier*.mailerinfo.com) to help avoid falling victim to this type of attack.

Another method is for the criminal to modify an email's headers so that an e-mail appears to come from the real address, but any reply will be diverted to another email address entirely (which would be revealed by looking at the metadata). Trust Companies should ensure they have SPF, DKIM and DMARC[6] enabled on their domains to make this type of attack more difficult.

In the more sophisticated attacks you see criminals taking control of people's email accounts - gaining access to another person's account using hacked or stolen credentials, or by compromising their computer or infrastructure – and then using it to send emails.

In relation to BEC attacks, watch out for a sense of urgency or poor spelling or grammar in the body of the email – and for last minute email account changes or bank account changes. Approval procedures for payments should always be applied rigorously without skipping any steps or giving in to pressure. They should also be stress tested to ensure they cannot be circumvented. They should set up a designated single point of contact with the companies to whom they make regular payments and ensure that multiple people sign off on high value transfers, by direct telephone call where necessary.

Another significant and closely related type of attack – impersonation – is seen by trust companies as the second biggest risk in the last year. Some 8% of those surveyed had experienced such an attack in the last 12 months. Impersonation is a social engineering technique where an attacker poses as a trusted person to steal either money or obtain sensitive or confidential information from a senior person within the company. Attackers often carry out extensive research on their victim using a range of publicly available information – such as information on the company's website or in people's social media profiles. They will often ask the person they are targeting to keep things confidential or private. To avoid attacks of this kind people within the organisation should be encouraged to restrict the amount they share about their employer on social media and consult a colleague within the organisation before actioning any unusual requests.

Ransomware, notwithstanding the increase in frequency and complexity of these attacks in recent year, was a lesser issue for trust companies – with only 1% of those surveyed seeing it as the main cyber and data security risk – and only 4% having experienced such an attack within the last 12 months (though that is still 1 in 25). In contrast in the CISO Report referenced above some 28% of CISOs perceived ransomware to be the biggest cybersecurity threat within their organisation/industry in the next 12 months. This can be reconciled in that, while ransomware attacks are perhaps less frequent than BEC fraud, the consequences for an organisation can be much more significant.

When it comes to defending against cyber-attacks, trust companies continue to lean in on people and procedures – with 28% investing in organisational measures in the last year and 10% increasing oversight of them. Again this chimes with the fact that the majority of CISOs are reported to see human nature as the biggest cyber security vulnerability within their organisation[7].

Technical measures are increasingly important to trust companies with 24% of companies surveyed investing in them and 21% investing in systems and incident response capability – such as incident response plans and wargaming. The criticality of ensuring that you have adequate planning in place to deal with an incident before it takes place and to make sure that such plans are integrated with your organisation's broader crisis management procedures cannot be overstated. In the heat of an incident there will be no time to iron out incompatibilities between different plans, to work out who is responsible for making decisions – or indeed to resolve differences in risk appetite between members of the leadership team. Mistakes in incident response can be very costly in terms of regulatory enforcement action, reputational harm and even litigation.

Cyber insurance is becoming increasingly important for trust companies too with some 6% of those surveyed increasing their cyber insurance cover in the last year. Again, in the CISO survey referenced, over half of global CISOs said they were confident that their policy would pay out when it matters most. However, the cyber insurance market is hardening. That means it can be more difficult to purchase cover, it is becoming more expensive and in some cases the scope of cover is narrowing (for example, some policies now contain broader 'war' exclusions which might bite in relation to nation state activity, which continues apace). This means that companies will have to take great care to check in advance of an incident that their insurance policies (including those beyond cyber, such as PI, crime, D&O, K&R, public liability or business interruption) will meet their needs – and to ensure that they do not inadvertently invalidate their insurance in the heat of responding to an incident.

---

1. Global C-Suite Series, 25th Edition, The CEO Study
2. CISO = Chief Information Security Officer
3. Proofpoint 2022 Voice of the CISO Global Insights Into CISO Challenges, Expectations and Priorities
4. The CISOs surveyed were from organisations of 200 employees or more across different industries in 14 countries.
5. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
6. SPF is sender policy framework (an email authentication protocol); DKIM is DomainKeys Identified Mail (an email authentication method designed to detect forged sender addresses in email) and DMARC is Domain Message Authentication Reporting) (a specification which authenticates emails by aligning SPF and DKIM mechanisms).
7. Proofpoint 2022 Voice of the CISO Global Insights Into CISO Challenges, Expectations and Priorities

ARTICLES IN THIS SERIES

KEY CONTACTS

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

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

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

GREIG ANDERSON
PARTNER, LONDON
+44 20 7466 2229
Greig.Anderson@hsf.com

LEGAL NOTICE