Adil Jaouhari

The security threats facing businesses, judged by industry experts

Ben Morley

06 July 2022 • 6 min read

SHARE

With technology ever more fundamental, and our collective reliance on it rising, the security of our tech is critical.

To establish the security issues technology business leaders and industry experts are most concerned about, *Computing* sent out a request for comment to senior personnel across these sectors.

They were asked "What's the most significant security threat to organisations right now, and what should organisations be doing to protect themselves?

Ransomware

Through the many responses, ransomware - where attackers disrupt an organisation's network and demand payment to unlock it - was the most cited threat by far.

In the last year, the US, UK, New Zealand, Australia and Canada have all warned of increased cyberattacks from various actors.

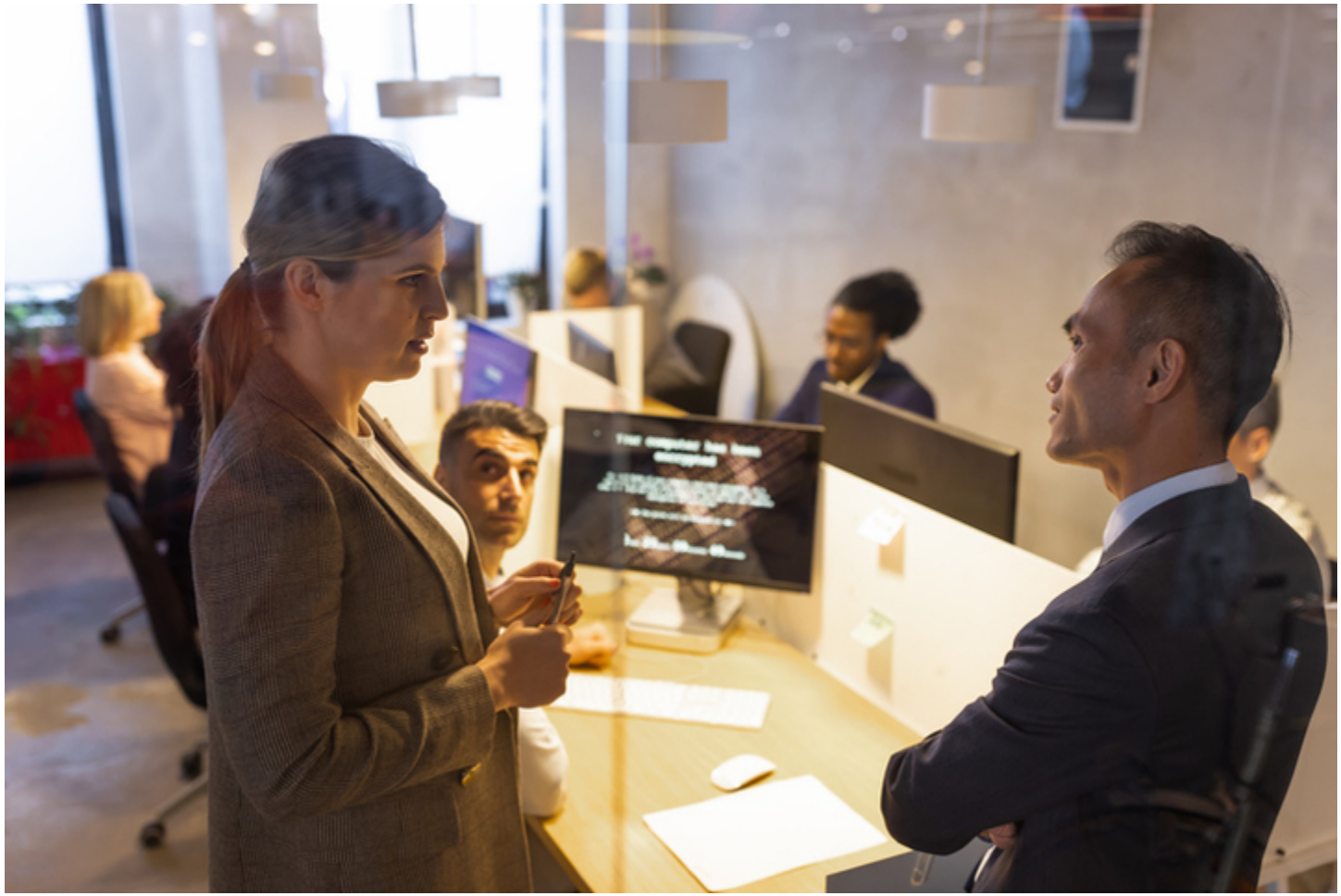
JBS, a top meat-packaging firm, was a major ransomware victim last year, and paid a total of $11 million to hackers.

Lee Wrall, co-founder of Everything Tech, commented that attacks are increasing: "The security issues that arose when the world began working from home during the COVID-19 pandemic were unprecedented, with malware and ransomware attacks increasing 358% and 435% respectively in 2020 as workers shifted to remote working.

"And according to research by the British Chambers of Commerce and Cisco, in the last year, one in 10 firms reported being a victim of a cyber-attack."

The European Union lists ransomware as the most worrisome malware threat. Global ransomware pay-outs are 57 times higher today than 2015.

Jamie Moles, an expert at cyber security company ExtraHop, said the risk exists for all companies: "Ransomware is extremely threatening to organisations, whether they be government entities, privately owned businesses, healthcare providers, or companies in charge of critical national infrastructure."



Saj Huq, CCO and head of cyber innovation at Plexal adds, "Over the past decade, there have been a number of large-scale cyber-attacks including the NotPetya ransomware attack that had ripples around the world. It would be dangerous to underestimate how much ransomware attacks pose a threat to UK businesses"

Plus, ransomware has not just increased in volume in recent years, but has also advanced in its complexity.

"Companies must deal with that fact that ransomware has evolved and diversified in recent years, as attackers are now deploying more targeted and sophisticated tactics," says , Oliver Tavakoli, CTO at Vectra.

Ransomware has also got faster. Rob Demain, CEO of e2e-assure, highlighted this as a major threat: "Organisations must wake up and realise that attackers are interested in their organisation, no matter how big or small it is…

"Organisations are also being given very little time to react - for example, Quantum ransomware made headlines in April due to having one of the fastest Times-To-Ransom (TTR) ever - only 3 hours 44 minutes."

Phishing

Many of the responses we read placed blame on phishing for tech insecurities.

Phishing involves a nefarious actor sending fraudulent emails or messages to a victim in the hope of compromising their security - such as via credential theft or ransomware installation. Spear Phishing, another attack mentioned by our respondents, sees hackers target specific people.

John Gilbert, general manager at Yubico, said "Phishing remains a top security threat to organisations as tactics continue to grow in volume and sophistication. Passwords don't stand up well to this form of attack because people might share them if they're tricked into thinking that's the right thing to do."

Steve Doyle, CIO at EDB, talked about the severity of the threat: "According to a 2021 report by Cisco, more than 90% of data breaches occur due to phishing, with hackers nefariously capitalising on the spirit of solidarity, empathy, and compas[illegible]t individuals have shown during the pandemic to hit small businesses and large corporations alike."

Often, the greatest vulnerability to phishing can come right at the end of the tech supply chain, as James Derbyshire, a browser isolation expert for Garrison, says: "The weakest point still remains with the users.

"Targeted, ransomware-based phishing attacks that encourage users to click on links in emails remains one of the most successful attack vectors and yet is one of the hardest to mitigate without just pulling the plug on their connectivity to the web."

Other notable threats

Beyond ransomware and phishing, a great many more security threats exist - for instance, Audience Hijacking. Patrick Sullivan, CTO at Akamai, said that "as the rates of online shopping continue to rise, online retailers are facing a growing challenge: audience hijacking…"

Sullivan describes the practice as "unauthorised ads injected into consumer browsers which lure shoppers away from online stores - disrupting the customer experience and inevitably leading to lost revenue."

However, away from external threats, some issues can arise internally, from businesses' own poor systems.

Nik Whitfield, founder and chairman at Panaseer, highlighted the real risk of inadequate systems. "The biggest security threat facing enterprises today is not Zero Days, but preventable cyberattacks that are let in through controls failures.

"Many enterprises already have the tooling they need to prevent or mitigate anything but the most sophisticated attacks, but still suffer breaches as tools aren't effectively configured or fully deployed."

What can be done?

Malware attacks are a fast-growing industry. Indeed, according to Verizons' Data Breach Investigations Report, attacks rose 13% this year: that‘s the fastest rise in five years.

However, the good news is there are many ways to secure against and counter hacks.

One such way, frequently recommended to us, was increased education for staff members and the general public.

Hans Vestberg, CEO and chairman of the telecommunications giant Verizon, said after the release of the company's Data Breach report "As we continue to accelerate toward an increasingly digitised world, effective technological solutions, strong security frameworks, and an increased focus on education will all play their part in ensuring that businesses remain secure, and customers protected"

Steve Doyle agreed: "Enterprise IT teams must always be looking for ways to monitor for and block such activity, and they must always be educating their users to ensure awareness and adoption of data protection best practices."

Likewise, Lee Wrall recommends expanded training: "IT security awareness training should be as commonplace as other areas of training offered by businesses, such as compliance training or Health & Safety. Businesses need to take online threats seriously and that starts with employees gaining greater awareness."

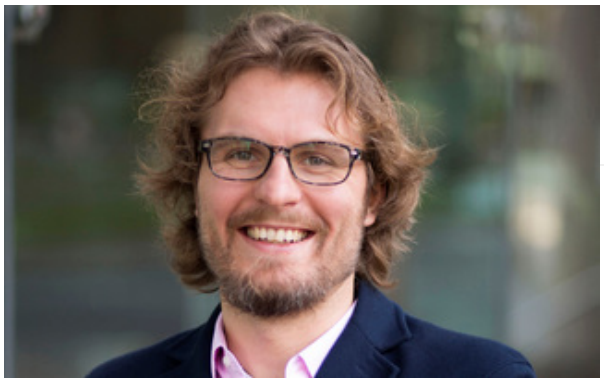
On a simpler level, some respondents promoted in-house internal upgrades. For instance, John Gilbert of Yubico said "In terms of mitigation, two-factor authentication (2FA) - for example SMS one-time passcodes and mobile authentication apps - help, as organisations can implement 2FA for remote working."

Nik Whitfield of Panaseer reiterated the importance of solving internal inefficiencies, and stressed the need to "prioritise and act upon the most business-critical vulnerabilities and avoid controls failures. [If so] we have a better chance of avoiding a serious incident and retaining our scarce security talent."

On a broader society-wide view, Saj Huq, CCO and head of cyber innovation at Plexal, raised the need to invest in companies that specialise in counter-malware technologies. "We need to fund early-stage startups that are working on this threat and provide them with insights from the government and the private sector that will help them develop their products."

While ransomware and phishing dominate headlines, many other threats exist. Modern businesses should invest in a range of solutions including staff training, updating legacy systems and counter-malware technologies to ensure proper protection.

More on Strategy



STRATEGY

Planning for success: how modern technologies can help organisations manage resources and remain resilient

STRATEGY

Video: Where does the office sit in the hybrid future?

Remote working has revolutionised how people interact with their jobs, but does the office still have a place?

STRATEGY

Staying cybersecure when 'bringing your own devices'

Kevin Curran, IEEE senior member and professor of cybersecurity at Ulster University, explains how to remain secure whilst enabling personal

PREVIOUS ARTICLE
Mark Fabes

NEXT ARTICLE
Interview: Lloyds Banking Group, Digital Tech... Leaders A... finalist