avoira

Cyber Attacks

What are the Risks and how can you mitigate against them?

This year's Cyber Security Breaches Survey contained a startling quote, one which is enough to extinguish the merest hint of complacency among those responsible for maintaining and securing private and public IT infrastructures.

Prepared by the Department for Science, Innovation & Technology (DSIT), the authors of the annual review reported:

"We estimate that UK businesses have experienced approximately 7.78 million cyber crimes of all types and approximately 116,000 non-phishing cyber crimes in the last 12 months."1

The survey also noted that one in two of all businesses had experienced some sort of cyber attack in the previous 12 months. For medium-sized businesses (the government classes those with a turnover of between £25-250 million as mid-sized) the figure rose to 70% and large ones higher still, at 74%.

The government itself is alive to cyber threats to our national infrastructure and economy. A Cyber Security & Resilience Bill was among the first pieces of proposed legislation to be unveiled in the King's Speech.

Due to be enacted next year, it is designed to extend legal oversight to more digital services and supply chains. In discussing the need for such legislation the DSIT specifically cites June's ransomware attack on London hospitals, a breach which not only led to the delay or cancellation of appointments and operations, but the release of sensitive data which one analysis suggests affected nearly one million patients.2

Incidentally, that number was calculated by CaseMatrix, a company which specialises in identifying, for legal firms, "potential class action cases arising from cyber incidents and data breaches." Where there's blame...

Counting the cost

Which brings us to the cost of cyber attacks, in terms of time, reputation and money.

Each year, IBM and the Ponemon Institute, an independent research and education facility that promotes best practice in information and privacy management jointly publish the global Cost of Data Breach report.

The 2024 edition is another sober read. It reveals that the average bill for a breach has risen 10% year-on-year to a record-breaking $4.88m. In the UK the cost was put at $4.53m, 7th in the global league table.

That figure included costs associated with detection and escalation, notification, post-breach response and lost business.

Lost business costs themselves – embracing factors such as system downtime, lost custom, regulatory fines and reputational damage – rose 11%.

The sectors suffering the highest losses included were the healthcare, financial, industrial, technology and energy industries.

Whilst the average time taken to identify and contain a data breach dropped to a seven-year low, it nonetheless still took a calendar-gobbling 258 days to clear up the mess; some nine months of IT forensics and fixes, time which might otherwise be spent supporting more productive organisational activities.

So, the cure is costly. Prevention – through cyber security products and, importantly, protocols – is a worthwhile investment. We'll look at actions you can take to mitigate against cyber risks shortly, but first let's take a look at just what those risks are.

Running Risks

Ransomware

Ransomware is a type of malicious software (malware) which prevents a user or organisation from accessing devices and systems through the encryption of files. The criminals behind such attacks then demand a ransom in exchange for an encryption key.

In order to demonstrate their own access to files, these gangs may release sample data. This what happened during one of the more high profile ransomware attacks to hit the UK this years, the targeting of Synnovis, a pathology partnership between medical testing provider and Guy's and St Thomas' NHS Foundation Trust and King's College Hospitals NHS Foundation Trust.

In addition to causing massive disruption to hospital and GP services, the hackers – Russian cyber crime group, Quilim – released some 400Gb of patient data onto the dark web.

Over three months later the repercussions of the June attack were still being felt. In September, Synnovis reported it had "successfully rebuilt the majority of core IT services" and that "the impact the cyberattack is having on local healthcare services continues to subside," adding, that "although regrettably we expect to feel its effects for some weeks to come."3

Whilst it's ransomware attacks focused on major corporates we hear about – they're more newsworthy by virtue of their size – SMEs are nonetheless a key target.

As SME magazine noted in October, smaller business are an increasingly attractive target as major organisations both tighten up their security and become less likely to meet ransom demands.

In making that claim the magazine cites data from the Cyber Security Breaches Survey – which shows SMEs do not prioritise cyber security as high as their larger counterparts - and analysis by cyber security outfit, Sophos. The latter showed that 28% of attacks mounted by LockBit, one of the world's most active ransomware gangs, targeted small businesses. Other major global gangs also see SMEs as significant targets.4

This news is particularly worrying for SMEs given the growing threat that ransomware presents. A key finding of the Cyber Security Breaches Survey was that:

"Ransomware remains the biggest day-to-day cyber security threat to UK organisations with attacks rising and the ransomware model continuing to evolve."1

Malware

Malware takes many forms and can perform different malicious actions. Apart from stealing deleting and/or encrypting data, these can include appropriating devices to crypto mine or to use them to attack other organisations.

Malicious software can also be used to obtain access to an organisations systems and/or services it uses. Another purpose is to direct use of fee-loaded services such as premium rate telephony which benefit the hacker.

Distributed Denial of Service (DDoS)

A DDoS attack involves flooding a server with malicious internet traffic in order to disrupt legitimate traffic and prevent access to a website and online services.

DDoS attacks involve the use of multiple connected devices – sometimes running into millions – with the sheer scale making them a challenge to tackle.

Cloudflare, a protective network which can sit behind websites, recently reported it mitigated against a record breaking DDoS attack that involved malicious requests which generated 3.8 terabits per second (Tbps) of traffic.5 It's worth emphasising that number; 3.8 trillion bits per second.

Whilst it's clear that attacks of that magnitude are targeted at major corporates, SMEs are far from immune from perpetrators' attentions. There are two reasons for this. Firstly, as mentioned before, SMEs can be seen as easier pickings due to cyber security being lower on priority lists. Secondly, SMEs can provide a gateway to larger corporates by virtue of being part of their supply chain, a weaker link.

If you're responsible for an SME's IT infrastructure it's worth pondering just what penalties your business might suffer should it be responsible for the breach of an important customer's systems.

State-sponsored attacks

The use of small-office and home-office (SoHo) devices by malicious actors to facilitate cyber attacks is an emerging trend.

Again, this is a weakest link approach, with protagonists taking advantage of relatively poor cyber hygiene to gain access to devices and use them to direct malicious traffic at private and public sector organisations.

The National Cyber Security Centre (NCSC) has warned that state-sponsored actors, most notably working for China, are increasingly deploying this technique.6

Phishing

Phishing – the use of scam emails or text messages – is easily the most common method of breaching are attacking IT security. Endured by some 84% of businesses1, these seek to entice recipients to release sensitive data, such as passwords or financial details, or enable malware.

Whilst phishing attempts may be crude, using, say, an anonymous greeting and a transparently false message, others can be highly sophisticated and targeted. The latter category may involve creation of a mirror site and the use of information related to the target organisation in order to bolster credibility.

Anyone can be a target for and a victim of phishing.

Earlier this year it was revealed that a number of Conservative and Labour MPs had been targeted, via WhatsApp, by a phishing attack. The source was unclear with Ciaran Martin, a former head of the NSCS telling The Guardian that: “It’s the sort of thing hostile nation states do, but unlike sophisticated cyber-attacks it doesn’t need nation state capabilities.

“So, absent of any specific evidence, there’s no basis to suspect any particular country. It could be anything from a hostile state to a bunch of jokers. The safeguards against are (a) not placing lots of unnecessary professional information in the public domain and (b) using common sense. If you can’t remember someone who claims to know you well, maybe it’s because you don’t know them.”7

Senior executives can be targeted for a business email compromise (BEC) attack. Unlike most phishing exercises, which deploy high volume and indiscriminate mail drops, BEC is targeted, seeking to gain a victim’s trust by impersonating someone they know.

Precisely because they do not disseminate mass mailings BECs can be harder for spam filters to detect, adding further credence to a mail which, being personally addressed and even containing previous correspondence, can appear legitimate.

Spoofed domains are another tactic adopted by BEC protagonists.

Botnets

A botnet is a network of comprised, malware infected interconnected devices, including routers, firewalls, webcams and CCTV cameras. These are used to conduct cyber attacks, including distribution of malware and, in particular, DDoS strikes.

In September the NCSC warned that a botnet comprising 260,000 devices has been operated by a Chinese company linked to the Chinese government since 2001.8 This particular beast incorporates a bespoke version of publicly available malware that automates compromise of devices and then activates connection to a command and control server.

This one botnet incorporated 8.500 compromised devices.9

Artificial intelligence (AI)

It would be counterproductive to ignore the undoubted and significant benefits that AI is and will bring to society. Equally though, it's important to recognise that, as with all technologies, it can be adopted by bad actors for malicious purposes.

The same powers – the ability to automate processes and speed data analysis – which are used for good, can be deployed to heighten and accelerate the threat of cyber attacks.

AI also has the capability to democratise cyber criminality by lowering the knowledge threshold required to commit, for example, ransomware attacks.10

Large Language Models (LLMs), which deliver such positive benefits to organisations deploying generative AI to enhance productivity, service, training, and much more, can also be abused.

As the NCSC notes, LLMs can impacted by data poisoning attacks in which an LLM's input data is corrupted to undermine the integrity of content and security. Such attacks are increasingly being used to secure data for exploitation by third-party applications and services.

LLMs can also be undermined through prompt injection attacks which "train" the model to generate offensive content, reveal confidential information or initiate other unintended consequences.11

Of course, the (considerably positive) flipside is that AI can and is being deployed to power sophisticated cyber defences which can analyse huge volumes of data, detect abnormal behaviours and automatically take actions to prevent or halt a breach or attack.

This neatly brings us on to the measures you might take reduce the possibility of unauthorised access , and/or minimise damage to your organisation's IT infrastructure and so protect its reputation, operations and bottom line.

Mitigating cyber risks

The cyber risk landscape is constantly evolving. It's important, therefore, that private and public sector organisations of all shapes and sizes take measures to insulate themselves from new criminal techniques and threats.

There are many things that can be done to mitigate risk.

Update & enhance

Whether a sole trader or multi-national PLC, it's vital to ensure that you constantly update soft and firmware to ensure that any vulnerabilities are addressed through patches or new releases. Such vulnerabilities might be found in an operating system, network switch, router, camera – pretty much any kit comprising or connected to an IT infrastructure.

Share knowledge

Cyber security is not simply the domain of IT professionals. Best practice and knowledge needs to be shared so that everyone is aware of, for example, how to create and protect a strong password, or spot and deal with a phishing or BEC attack.

Learn, implement, thrive

Not only can adopting good cyber hygiene help protect your business – it can help you attract new custom.

Completing the government-backed Cyber Essentials or Cyber Essential Plus schemes is more than a good start. These cover five key cyber security controls: firewalls, secure configuration, access control, malware protection, security update management.

As well as providing invaluable direction, securing Cyber Essentials accreditation signals to customers and potential customers that an organisation takes protection of its systems and data – which may include theirs – seriously. Some public sector bodies also require their suppliers to hold certification.

You can learn about Avoira's own journey to Cyber Essentials Plus accreditation here. If you're interested in securing either level of accreditation you can also contact us for insights, advice and support.

Multi-factor authentication (MFA)

MFA, or two-factor authentication (2FA) can be a relatively simple way of significantly enhancing cyber security.

It involves a user being required to enter more than just a password to access an account or service. This might involve inputting a code generated by an authenticator app, answering a question, completing an image-based questionnaire or submitting a fingerprint.

Despite its relative ease of use, MFA can meet with resistance. It's important, therefore, to explain the benefits it brings.

Beverley Bryant, strategic advisor in the frontline digitisation team at NHS England, has noted that the London hospitals breach referenced earlier could have been prevented had 2FA been in place, and that it "is the single biggest deterrent we can put in" to ensure [NHS] trusts are more cyber resilient and minimise the risk of attack."

She noted too that whilst some clinicians may complain about the implementation of 2FA, "they soon get over it."12 There is, no doubt, a wider lesson to be learned from that insight.

Cyber security solutions

There are, of course, a multitude of cyber security solutions on the market, each offering differing strengths and selling points.

These include ESET PROTECT, a customisable platform designed specifically for small businesses, managed from a cloud console, easy to deploy and offering excellent malware protection.

Mimecast is particularly good at warding off phishing, BEC attacks and the potential compromise of collaboration tools such as Microsoft Teams, One Drive and Share Point. It can be integrated with a number of security technologies including Google SIEM, Microsoft Azure Sentinel.

When it comes to ransomware, our engineers are particularly enamoured by Bullwall RansomCare, a 'Last Line of Defence' solution, so called because it sits behind other cyber-security solutions, from firewalls through to sophisticated Extended Detection and Response (XDR) technologies.

Once it detects encryption taking place, in real-time, it rapidly isolates the affected user and device to prevent the spread of encryption to any other users or storage areas. Additionally it simultaneously isolates the hostile client seeking to encrypt data.

Managed service provision (MSP)

MSPs can greatly assist resource-limited organisations to keep on top of product updates and optimise security. An MSP will be contracted to monitor and manage networks and infrastructures, and manage specified tasks such as data storage, firewalls and Security as a Service (SECaaS – cloud-based security technologies).

Day-to-day, these services are typically provided remotely, but may be supported by on-site interventions as required.

MSPs can deliver highly cost-effective and anxiety reducing services which free time and resource to empower organisations to focus on their core activities.

If the concept is of interest, Avoira offer flexible and bespoke managed services contracts.

Useful resources

Cyber hygiene

- The Essential Cybersecurity Kit for SMBs
- Cyber Aware
- Protecting bulk and personal data
- Would you benefit from a Free IT & Network Audit?

Malware and ransomware

- Mitigating malware and ransomware attacks
- A guide to ransomware

Phishing & Business Email Compromise

- Phishing: Spot and report scam emails, texts, websites and calls

Distributed Denial of Service

- Denial of Service (DoS) guidance

Multi-Factor Authentication

- What is multi-factor authentication?
- Multi-factor authentication for your corporate online services

Securing your future

If you need further information or advice on how to better secure your organisation's devices and data, please don't hesitate to contact us.

We are also able to offer free online and onsite demonstrations of key solutions, together with no—strings cyber security audits.

☎ 0333 001 5151

✉ info@avoira.com

🌐 avoira.com

The authors qualify this statistic, stating "these estimates of scale will have a relatively wide margin of error". Source: Cyber Security Breaches Survey, Department for Science, Innovation & Technology, April 2024. 2. The Record, 16 September 2024. 3 Source: Synnovis, 13 September 2024. 4,. The 2024 Sophos Threat Report: Cybercrime on Main Street, 12 March 2024. 5. Source: The Hacker, 04 October 2024. 6. Source: National Cyber Security Centre, 09 July 2024. 7. Source : The Guardian, 04 April 2024. 8. Source : National Cyber Security Centre, 18 September 2024. 9. Source: Joint Cybersecurity Advisory, 18 September 2024. 10. Source: National Cyber Security Centre, The near-term impact of AI on the cyber threat, 24 January 2024. 11. National Cyber Security Centre, AI & Cyber Security: what you need to know, 13 February 2024. 12. Source: Digital Health, Two-factor authentication may have stopped Synnovis cyber attack', 25 September 2024.