Exploring Organisational Experiences of Cyber Security Breaches

Report

Ipsos

Contents

1 Glossary

Term	Definition
Cyber security	Cyber security includes any processes, practices or technologies that organisations have in place to secure their networks, computers, programs or the data they hold from damage, attack or unauthorised access.
Cyber attack	A cyber attack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation.
Security breach	A security breach is any incident that results in unauthorised access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
Outcome	A negative outcome of an attack involved a material loss from an organisation, such as a loss of money or data.
Impact	A negative impact on organisations did not have to involve a material loss. This could be issues relating to staff disruption or implementing new measures in the organisation.
Micro business	Businesses with 1 to 9 employees
Small business	Businesses with 10 to 49 employees
Medium business	Businesses with 50 to 249 employees
Large business	Businesses with 250 employees or over
Low-income charity	Charities with an income of less than £100,000
High-income charity	Charities with an income of £500,000 or more
Very high-income charity	Charities with an income of £5,000,000 or more
Cloud computing	Cloud computing uses a network of external servers accessed over the internet, rather than a local server or a personal computer, to store or transfer data. This could be used, for example, to host a website or corporate email accounts, or for storing or transferring data files.
Denial-of-Service Attack (DoS)	A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
Distributed Denial-of-Service Attack (DDoS)	A Distributed Denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Malware Malware (short for “malicious software”) is a type of computer program designed to infiltrate and damage computers without the user’s consent (e.g., viruses, worms, Trojan horses etc).

Managed Service Provider (MSP) A supplier that delivers a portfolio of IT services to business customers via ongoing support and active administration, all of which are typically underpinned by a Service Level Agreement. A Managed Service Provider may provide their own Managed Services or offer their own services in conjunction with other IT providers’ services.

Patch management Having a policy to apply software security updates within 14 days of them be

Penetration testing Penetration testing is where staff or contractors try to breach the cyber security of an organisation on purpose, in order to show where there might be weaknesses in cyber security.

Personally-owned devices Personally-owned devices are things such as smartphones, tablets, home laptops, desktop computers or USB sticks that do not belong to the company, but might be used to carry out business-related activities.

Phishing Fraudulent attempts to extract important information, such as passwords, from staff with infiltration through a link or attachment sent via email.

Smishing A ‘smishing’ attack is a form of phishing in which the actor uses a compelling text message to trick targeted recipients into clicking a link and sending the actor information or downloading malicious programs to a smartphone.

Social engineering Fraudulent attempts to extract important information, such as passwords, from staff with infiltration through an impersonation attempt of the organisation.

Spear phishing Spear phishing is a phishing method that targets specific individuals or groups within an organization.

Ransomware A type of malicious software designed to block access to a computer system until a sum of money is paid.

Removable devices Removable devices are portable things that can store data, such as USB sticks, CDs, DVDs etc.

Restricting IT admin and access rights Restricting IT admin and access rights is where only certain users are able to make changes to the organisation’s network or computers, for example to download or install software.

Smart devices Network connected devices, like personal assistants, locks, alarms, or thermostats.

Threat intelligence Threat intelligence is where an organisation may employ a staff member or contractor, or purchase a product to collate information and advice around all the cyber security risks the organisation faces.

Two-Factor Authentication Two-Factor, or Multi-Factor, Authentication is an electronic authentication method in which a user is granted access to a network or application only after successfully presenting two or more pieces of evidence to an authentication mechanism (e.g. a password and a one-time passcode).

Vishing Voice phishing, or vishing, is the use of telephony to conduct phishing attacks

2 Research objectives

In March 2021 the Department for Digital, Culture, Media and Sport (DCMS) published the Cyber Security Breaches Survey of UK businesses, charities, and education institutions as part of the National Cyber Security Programme. (The study was re-run in 2022 and a new report has now been published). The findings help businesses and organisations understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the Government to shape future policy in this area.

Building on this earlier research, in January 2022 DCMS commissioned an in-depth qualitative study with a range of businesses and organisations which have been affected by cyber security breaches. The specific aims of this research were as follows:

- Understand the level of existing cyber security before a breach
- Determine the type of cyber attack to which the organisation was subject
- Understand how businesses and organisations act in the immediate, medium, and long-term aftermath of a breach
- Investigate the impacts upon the business or organisations immediately and into the future
- How cyber security arrangements have changed in the wake of a cyber breach

3 Methodology

Fieldwork was conducted over the period 23 February to 21 March 2022.

Qualitative interviews were conducted via Microsoft Teams with employees across ten organisations that have between them experienced a variety of types of cyber security breach in the last three years.

To build a detailed, rounded picture of the breach, interviews were conducted with at least two employees per organisation. Interviews were typically conducted with someone in an IT or cyber security role who dealt with the breach, and another member of staff who was directly impacted by it. Due to the sensitive nature of the issue interviews were conducted separately.

Participating organisations varied by size, sector and type of breach as is detailed in the table below:

	SIZE	JOB ROLE	BREACH	IMPACT
1	Small	IT Manager General Manager	Spear Phishing Attack	Financial, employee stress/dissatisfaction/attrition
2	Medium	Head of Digital Compliance Officer	Spear Phishing Attack	Financial
3	Large	Chief Information Security Officer Security Operations Lead	Smishing Attack	Financial, customer dissatisfaction
4	Large	IT Director Business Systems Technician	Denial-of-Service Attack	Financial, employee stress/dissatisfaction/attrition
5	Micro	Chief Executive Finance Director	Denial-of-Service Attack	Financial, customer dissatisfaction, reputational damage
6	Medium	IT Manager Managing Director	Ransomware Attack	Financial, customer dissatisfaction, reputational damage
7	Large	Chief Information Security Officer Security Operations Lead	Denial-of-Service Attack	Financial
8	Medium	Group IT Director Director of Finance Operations	Ransomware Attack	Financial, customer dissatisfaction employee stress/dissatisfaction/attrition
9	Small	Head of Strategy Risk Manager	Spear Phishing Attack	Financial, employee stress/dissatisfaction/attrition
10	Large	IT and Transformation Director IT Manager	Ransomware Attack	Financial

The experiences of participating organisations are detailed in the ten case studies in section 4. We would stress that the case studies present the facts of the various incidents as reported by the organisations, and they do not pass judgement or comment upon the sufficiency or suitability of the security provisions in place within each organisation.

4 Key findings

The ten organisations that participated in this study have all suffered a serious cyber security attack within the last four years. The similarities between them largely end there, as the organisations vary widely in scale, level of IT resourcing, cyber security measures in place prior to the attack, and their response to the attack.

Nonetheless, several themes do emerge from this disparate set of study participants. Firstly, there was a consensus that cyber-crime is a significant and growing business risk, with cyber attacks increasing in both volume and technical sophistication. Knowledge of this fast changing 'threat landscape' did, however, vary significantly between study participants.

In response to these increasing levels of risk, nearly all participants acknowledged the need for ever greater levels of vigilance and investment in cyber-security, as the controls that were appropriate a few years ago are now seen as less effective. That said, while interviewees from medium and large organisations said they tended to have formal plans in place and budget allocated for further cyber security investment, interviewees from smaller organisations were more likely to assert they did not, largely citing resource constraints. Their response to the perceived growing cyber security risk therefore appears to be largely piecemeal and reactive.

Unsurprisingly, given the broad mix of organisations included in the study, the cyber security arrangements and technology deployed also varied enormously. Nevertheless, nearly all participants indicated that their organisation took cyber security 'seriously' prior to the breach; indeed, most characterised their arrangements as on a par with or better than their peers.

The majority felt their organisations put more of an emphasis on technology than employees to stay secure. For some, technology was a tool to 'help people do the right thing', reflecting the widespread notion that people and culture are more of a cybersecurity 'weak spot' than the technology deployed at their organisation.

Participants also reported varying levels of support and interest in cyber security from the leadership teams within their respective organisations. Encouragingly, most said that their leadership had grasped the importance of cyber security and was increasingly supportive of investing in it, with some already treating it as a 'board level business problem'. At the same time, not all were sure that their leadership teams fully understood the 'scale of the threat', or the 'cultural transition' required to meet the growing cyber security challenge.

Therefore, for numerous participants, one positive outcome of the breaches they experienced was in demonstrating that 'these cyber threats are real' to leadership, underscoring the importance of cyber security. Consequently, for many organisations in this study, leadership became more engaged in the cyber security challenge post-breach and has since demonstrated more serious intent to help the organisation improve.

Turning to the breaches themselves, in most instances organisations in the study were able to determine the cause and fix the 'weakness', often drawing on the support of external vendors. For some participants, the breach was a cause of considerable personal stress and upheaval – some of which has proved long lasting - while others were more sanguine, characterising the episode as an inconvenience rather than a calamity.

Once their breach was fixed, relatively few organisations in the study tried or were able to accurately quantify its financial impact (although most participants were able to provide broad estimates, typically covering the cost of lost sales, employee downtime and IT consultancy).

Similarly, very few organisations in the study implemented a formal 'lessons learned' process in the aftermath of the breach. Despite this, most participants felt that they were now better protected than prior to the attack, having since strengthened aspects of their cyber security technology, policy, or staff training.

The role of the UK government in addressing cybercrime

Some participants spoke positively about the support available from government in relation to cyber security as well as its wider role combatting cybercrime. This mostly reflected their experiences working with the National Cyber Security Centre (NCSC) or other bodies, the information they have received from Government agencies or their views on the positive impact of General Data Protection Regulations (GDPR).

> *I think GDPR was a very good thing as it made businesses comply to a standard which was agreed universally. GDPR has caused businesses to spend a lot more on data and tracking and I think businesses now understand they have a responsibility to keep their data secure*
>
> *IT Manager, large organisation*

> *I'm impressed with the amount of information that is available [from government] and directed at small, medium and large organisations…. Perhaps they should target the non-technical CEOs [Chief Executive Officers] more proactively as I feel a lot of their communications are simply preaching to the converted*
>
> *IT Director, large organisation*

> *Overall, we found the government agencies very useful as there was somebody there you can talk to, and the NCSC actually told us what had happened to our system.*
>
> *IT Manager, medium organisation*

When asked what else the government should be doing to address the growing cyber security challenges faced by organisations, around half of the interviewees who participated in the research thought it should focus primarily on raising awareness and education:

> *There are probably hundreds of other companies out there like us who are not aware of what can happen…. So I think it is important that the government builds awareness. We are members of the BVLRA [British Vehicle Rental and Leasing Association, an organisation which consults with the government to maintain standards and help members deliver safe, sustainable and affordable road transport to millions of customers and business] who give us updates on what is happening in the industry …. I think they should include something on cyber security provided by the government.*
>
> *General Manager, small organisation*

> *There's not a lot of awareness amongst the public. I do not see much in the media on cyberattacks…. And we're not really hearing anything on this as a business. So, I think some sort of cyber crime prevention campaign roll out wouldn't go amiss.*
>
> *IT Manager, small organisation*

Some participants felt that the government's focus should be on raising awareness amongst the general public rather than companies, as 'consumers keep getting hit' and they need to 'stop people being compromised'.

A minority of participants did not, however, see a pressing need for further government involvement in improving cyber security, either because ‘people don't know what cyber security is and they won't listen’, or because the government is not a credible source of advice for businesses:

> *I don't think there's much more the government should be doing as cyber security is down to the individual company and who they are employing. It is the company's responsibility to make sure people are adequately trained and competent when it comes to security, and I think legislation is already in place.*
>
> *Head of Digital, Medium sized organisation*

> *The expertise I bring in comes from commercial sources. So, I have not taken the government seriously as a source of what to do.*
>
> *IT and Transformation Director*

Some interviewees asserted that government needed to take cyber security ‘more seriously’, suggesting harsher punishments for cybercrime as a form of a deterrent, and by ‘acknowledging that foreign states are behind some of these attacks’ and addressing this.

Finally, two out of twenty interviewees who participated in this research requested more regionally based cyber awareness training, while one other called for the government to do more to ‘bring together academics, government, and business as this [cyber security] collaboration is hugely important’.

5 Case studies

Case Study 1

Background

Private sector organisation with 10–49 employees. Interviews were conducted with the General Manager and IT Manager.

In August 2021, the organisation was hit by an email phishing attack. The unknown actor was able to gain control of its Microsoft 365 administrator account and used this to send phishing emails containing Malware to most of the organisation's external clients and contacts.

Level of existing cyber security before the breach

Prior to the breach, due to financial and resourcing constraints, many of the organisation's IT functions, including security, were outsourced to a local provider located in the same town. According to the General Manager, the senior management of the business had given little thought to the possibility of a cyber breach as 'we thought our provider at the time had it all covered, and we were watertight'. Nonetheless, in retrospect they feel they were 'unaware' and 'naive'.

The IT Manager also characterised senior management as largely oblivious to potential cyber threats, and 'not really aware of what is going on' with little interest or knowledge of IT in general, and they described staff overall as not particularly 'computer literate'. Despite this, the IT manager 'expected the protection to be pretty good as it is cloud based' and was 'pretty happy' with the set-up as they trusted their outside provider. They also described the business as 'a little ahead of our competitors and a step above in terms of security', with in place, as well as anti-virus software and 'some anti-crime software'.

The business had little or no formal cyber security processes or staff training in place, and no cyber contingency or emergency planning procedures. In the IT manager's words, 'I'd been thinking more about recovery from disaster so for example we had cloud backups of the system in place in case the building caught fire… I was thinking more about these sorts of physical attacks rather than cyber attacks'.

The breach and the organisation's immediate response

The breach came to light after the General Manager emailed an invoice to a customer on a Tuesday afternoon in August 2021. During a conversation with this customer the next morning, it became evident that the email had been intercepted and bank details changed on the invoice. Consequently, the customer had unwittingly transferred funds into an unknown bank account. (These funds were promptly retrieved by the customer's bank.)

Once aware, the IT Manager immediately contacted the IT support company only to be disappointed by their lack of responsiveness as 'they took quite a long time to get back to us. It was about two or three hours'. In the meantime, the organisation accessed their Microsoft 365 control centre and noticed that it had been compromised. The IT provider then intervened and 'after a few hours they said it was all sorted and assured us that the door was shut'.

The next morning (Thursday) the IT Manager again accessed their 365-control centre and noticed that 'things had changed as we should only have one 365 admin account but there were two or three of them'. The IT provider investigated this and said that the actor was in again. Soon after, they became aware that the actor had used the account to 'spam out to all our clients a phishing email. This was quite a few thousands of emails, after which the phones were lit up as it absolutely snowballed'. The email contained malware in the form of a PowerPoint attachment. The IT provider was eventually able to shut out the attacker and secure the 365 account.

On Thursday, as soon as they became aware of the phishing emails, the General Manager alerted all staff to the issue so they could tell customers not to open emails. Soon after this, the IT provider emailed all clients with a 'do not open our previous email' message.

That day, the General Manager and Finance Director also informed their bank and finance houses of the breach, thinking they could have been affected. Nonetheless, 'some had systems in place to stop the email and actually sent it back to us flagging it as malware'. Furthermore, the General Manager and their team had to speak to 'a lot' of customers.

The identity of the attacker was never established, although the organisation was quickly able to determine the cause of the breach with help from their IT provider. According to the GM, 'it turned out that our old IT provider had sent a gateway password in an email which was then hacked and allowed us to be infiltrated… It should never have been sent, other providers who I talked to afterwards were aghast that it was'.

In addition, the IT manager identified further vulnerabilities during the Thursday and Friday of the week of the attack. Having read up on Microsoft 365 he found 'a lot of things hadn't been set up correctly by our provider. But when I contacted our provider, they weren't apologetic…they tried to bamboozle me with tech talk'.

Impacts upon the organisation

The organisation did not quantify the financial cost of the attack but acknowledged that aside from the downtime due to staff 'answering the phones and sending out emails to say do not open the phishing email', it was 'not huge'. Similarly, the damage to their reputation and customer relationships was not regarded as long lasting, nor was any impact on staff morale.

At a personal level the GM found the experience 'devastating' and akin to an assault, not least because the malicious email campaign used their email address and some of their personal data was also stolen. Added to this, they felt 'embarrassed' that they had exposed clients to increased risk of a cyber attack. For the weeks that followed they felt they were 'walking on eggshells'.

The IT Manager also found the experience distressing, recalling that 'I'd set up the infrastructure. It sits on my shoulders, so I had to take it on the chin from our directors and I felt I'd let myself down. It had a real impact as then I started to question everything that I did… it really got me down to be honest'. They did however find senior management to be supportive throughout the period of the breach.

How cyber security arrangements have changed in the wake of a cyber breach

Both interviewees noted that the breach has made the organisation more vigilant, especially at a senior management level, and had prompted it to review and improve its cyber security arrangements and external support. The organisation has not, however, made formal changes to its internal policies, although some of its processes have evolved.

Having established that the complacency of their existing IT provider had made them vulnerable to the attack in the first place - a failure compounded by their slow response during the breach – the General Manager and IT Manager were able to get immediate sign off from their Board to begin a tendering process for a new IT provider.

The IT manager identified seven companies who were invited to tender for the new contract. Each company was interviewed in person, resulting in a shortlist of two providers both of whom offered a similar approach. A key selection criterion was to find a 'partner' who would offer responsiveness. Consequently, they opted for the most local of the two shortlisted providers 'as we wanted easy access to them and people who could come in to help us'.

In the words of the General Manager, the new provider is 'on the ball' and 'transparent'. Their first task was to rebuild the organisation's 365 account structure with the correct security. They also implemented Multi Factor Authentication (MFA) for all Microsoft logins and tried to raise employee awareness by sending out regular test emails to see who would open potentially fraudulent messages. In addition, there is now a process in place for employees to send potentially fraudulent emails for screening to the IT provider.

The organisation does not currently have any cyber security certification but is working towards Cyber Essentials Plus, having already made further investments in hardware, software and a new systems. In the words of the IT manager, 'I feel a lot happier now and I think your everyday actor would struggle to get through our security with so much in place'.

Case Study 2

Background

Private sector organisation with 10-49 employees. Interviews conducted with the Head of Digital and the Compliance Manager.

In October 2021, the organisation was hit by a Distributed Denial-of-Service (DDoS) attack from an unknown actor that affected its e-commerce and Customer Relationship Management (CRM) platforms.

Level of existing cyber security before the breach

The Head of Digital is an experienced developer with responsibility for all IT infrastructure and security, as well as the organisation's fast growing ecommerce channels. They characterised the organisation as 'tech savvy enough to have covered the basics' prior to the breach. Indeed, compared to other organisations of a similar size, they regard it as having been 'bang on the average or even a little bit better as we're a fairly tech forward company for someone in our industry'.

All IT services were cloud controlled so they could 'shut them off if we see strange activity'. Furthermore, key information was kept on a firewalled and separate network that only two people have access to. Therefore, if a 'laptop was stolen someone would only have access to very limited information'.

Both respondents did however point out that cyber security was 'not really on the minds' of directors or employees, the Head of Digital noting that 'it has been an effort to get them into the basics with for example two factor authentication'. Consequently, the Head of Digital regarded internal policies in relation to cyber security as generic and 'basic', although they reflected that in their experience this was very much the norm - 'it is the same everywhere they just use a standard template that [they] downloaded from a government website'.

The Head of Compliance was more confident about the internal policies and processes in place, noting that prior to the breach they were not personally worried about the prospect of a cyber breach as they were 'quite proactive'. In Strength, Weakness, Opportunity, Threat (SWOT) analysis they had identified a cyber attack as one of the 'top five threats' so they had looked at how to mitigate it, although so far had only documented the procedures for reporting it.

The breach and the organisation's immediate response

Since 2018, there had been a few instances of 'people opening your standard spoof and spam emails', but none of those were judged to have had a business impact. The only significant cyber breach occurred in October 2021 and was an attack on the organisation's main web server. This is the single instance 'where any damage was done', although there was not a loss of client data or any other information.

The breach was handled solely by the Head of Digital. They described it as 'a massive inconvenience for me, but no one else really knew what was going on'. As they were the sole employee in the organisation with the skills and knowledge to resolve the breach, they did not involve colleagues.

The organisation uses an open-source e-commerce plugin for WordPress as its e-commerce platform. The Head of Digital described a vulnerability in commerce plugin that 'enabled people to run a script remotely and if it wasn't patched, they could import custom code into the software'.

Although they had already patched this vulnerability, a script ran continuously on their site writing 'fake users' into the organisation's database (in essence creating 'about 500 or so' user accounts per minute). This 'overwhelmed' their server, so they faced a DDoS. The attack targeted the organisation’s US ecommerce platform, but as this ran from the same resource as the domestic ecommerce site ‘the UK cracked as well’.

The organisation’s entire e-commerce and CRM platform were down for approximately five hours, during which time they could not take online orders. The Head of Digital found out about the issue on the train home from work. They resolved it that evening by ‘cleaning up the database’ and then ‘going through our logs manually to ensure that nothing had been read and no data taken’. They were soon confident that there was no data breach.

The Head of Digital then focused on ‘blocking the bad IPs [Internet Protocol addresses] that were the source of the attack’. These were constantly changing, and this was the most time-consuming aspect of the breach response. Fortunately, the attacks were being run from a ‘bot farm on an Azure platform’ which made it easier to deal with ‘as all the IP addresses were in a certain range so we're only facing attacks from about 15 IP addresses at a time which made them easier to block.’ The Head of Digital reported the attack to the vendor providing the Operating System, but has not received a reply so does not know if the vendor took action against the bot farm. They report feeling frustrated at the lack of communication.

Over the ensuing two or three weeks the organisation faced a ‘few minor attacks’, but these petered out. During this period, nothing was reported to official bodies or to the organisation’s customers as no data was lost.

Senior management were kept informed of the situation but were not directly involved in its resolution or indeed particularly alarmed by events. As the Head of Compliance reflected, ‘the directors are very engaged with us and they know what is going on and trust us. I think there is a culture where it is okay to make mistakes as long as we learn from them’. As the Head of Digital expanded, ‘they are lucky that I am an inhouse developer so I was able to stop it in its tracks. If they didn't have me, they would have [really been in trouble]’.

Impact upon the organisation

Although it was a ‘pain’ for the Head of Digital, the impact on the organisation was minor. It was not formally quantified, but they estimate that there was very little financial cost in the form of lost sales and no damage to its reputation or customer relationships.

The Head of Compliance noted that the breach served to ‘raise awareness for me personally and it has made me want to look into cyber security and I have actually requested further training so that I can have more input and I am able to give more support in this area”.

How cyber security arrangements have changed in the wake of a cyber breach

The Head of Digital wrote a report on the breach which was reviewed at a senior management meeting. The organisation then made a ‘significant investment to maintain better services’ and is now hosted on Google cloud which is more expensive than their previous set-up – ‘about four times as much’. It has also separated its US and other international e-commerce sites from its main UK site so that if one is affected by an attack, it will not impact them all.

In addition, they are launching a new ecommerce platform later this year and will not be using a standard platform but are instead developing it in-house as, in the words of the Head of Digital, ‘the more commonly used a platform is, the easier it is to hack into so it is better to do the development yourself’.

The Head of Digital views the current set-up as ‘fairly secure’ as someone externally would now find it difficult to crack. Their main exposure is if someone ‘gains access to a laptop and sends out ransomware by email from us’.

Case Study 3

Background

Private sector organisation with over 250 employees. Interviews conducted with the Chief Security Officer (CSO) and Head of Security Operations (HSO).

On 3rd July 2021, the organisation was hit by a DDoS attack. The unknown actor attacked the organisation's third-party host provider which led to its web site and e-commerce platform being inoperable for 41 minutes. This resulted in significant financial loss to the organisation.

Level of existing cyber security before the breach

This is a large and complex organisation with a sizeable IT footprint. It is responsible for logistics, manufacturing and the e-commerce platform for numerous franchisee groups who operate over 1,000 retail outlets. Consequently, prior to the breach it had a significant cyber security resource in place led by the CSO who reports to the Board and is responsible for everything to do with cyber risk and information risk management

According to the CSO, when they joined the organisation in 2020 its security was 'variable'. Since then, it has gone from 'immature' to 'quite good', but it is still improving. Before the attack, the CSO characterised the organisation as being 'in a good place from a website protection point of view' as we do 'lots of testing' and 'front end deflection work in the cloud'. So, if they faced a distributed denial-of-service (DDoS) attack against their platform it would have been deflected.

The CSO does not, however, benchmark cyber security against peers. They see no value in it, stating 'I am building controls appropriate to our threats… also who do we benchmark ourselves against as we are an e-commerce platform and a logistics platform and a manufacturing business'.

In recent years, the organisation has weathered two attacks that have had a business impact. Beyond these, it is 'constantly being scanned, probed and prodded' according to the CSO. But, in the words of the HSO, 'we have a lot of mitigations and controls to stop them being successful', including Acronis for protection of all of their externally facing assets (i.e., web firewall DDoS geo blocking).

The breach and the organisation's immediate response

The DDoS happened 'five minutes into the England-Ukraine game', which kicked off at 8pm on 3 July 2021. It was an attack on the organisation's third-party host provider not directly on its website which is less vulnerable due to its DDoS protection software.

The organisation knew instantly of the attack as its website went down, and 'the only thing we did not know was why it happened'. The organisation's incident response team was immediately spun up and the website was back up and running in under 50 minutes. During that period, customers were unable to place orders and the company could not check their online systems. At about 3:00am the next morning the unknown actor tried to take the system down again, but the impact was 'negligible' according to the HSO.

Post-event on the Monday morning (5th July) the cyber security team had a meeting to determine what happened and 'how did we miss that gap?' It then took some time to identify the root cause of the issue as initially the third-party host provider reported that it was not a DDoS attack. Nonetheless, the organisation went into its login systems and conducted some analysis, finding 'plenty of evidence' that it was a DDoS attack 'so we told them this and they said "yes you are right"'. The organisation was the only entity affected by the attack on the third-party host provider as they have a dedicated infrastructure on it.

An IT consultancy was commissioned that week to further investigate the incident. According to the HSO, their recommendations were that it was ‘a missed configuration and a process had not been followed properly at the data centre…. They identified that there was an onboarding processing issue at the third-party host provider and there was not enough due diligence done by them.’ Consequently, a device slipped through the net and did not have DDoS which enabled the unknown actor to attack the infrastructure. Although the HSO thought the consultants did not tell them anything they did not already know, ‘it was useful to have validation from a fresh set of eyes….After that review they presented their findings to us and the provider, so that was constructive’.

No one was informed of the incident outside of the organisation and its franchisees because the CSO and their team did not classify it a security breach in terms of data integrity or confidentiality, therefore they saw no mandatory notification requirement.

Impacts upon the organisation

The CSO was informed of the breach about 30 minutes into the event. They were then on telephone calls with the third-party host provider, ‘so it was only down for 11 minutes that I was aware of’. Consequently, they did not find it especially stressful. Furthermore, the CSO reports directly to the Board who they characterised as highly supportive. When the CSO joined the organisation they told the Board that cyber security ‘will take time to fix and there are a lot of holes and risk of a breach that will be there for some while’. Consequently, at the time of the breach the Board understood that ‘we are not yet bulletproof’ and the CSO was not to blame.

The HSO found the experience ‘very stressful’ on Saturday night when the breach occurred because they worked until 2:30am on Sunday morning and then got up at 6:00am on Sunday ‘as at that point we had not found the reason, the root cause yet’.

The financial impact on the organisation was significant with lost revenue estimated to be in the range of £500,000 due to it not trading for around 50 minutes on a Saturday evening. Added to this, there was ‘a time and effort operational cost’ totalling hundreds of IT hours with ‘people stopping their day job to be engaged in the breach…. People getting involved in security when they should be for example helping with new store openings, and then after the immediate breach there is a lesson learned process.’

In addition, the organisation’s franchisees ‘are very vocal so we had numerous phone calls’ during the time when the e-commerce platform was down.

How cyber security arrangements have changed in the wake of a cyber breach

The organisation has stayed with their third-party host provider in the short-term as ‘it is easier to fix what you have got rather than finding a new one that may be no better’, and they have also benefited from improvements in their account team at the provider. The organisation has, however, made changes so that all their third party infrastructure is always under DDoS protection (specifically, they have revised the change management procedures so that when putting in new infrastructure ‘it immediately has top level protection’).

The CSO however characterises this as a ‘short-term quick win’ to ensure there is no recurrence. In the longer term they are working on ‘bigger transformation’ as ultimately their website will have a new home - ‘a lot of what we are doing are compensation measures and secondary measures rather than addressing the root cause as there is no point doing that as we will be changing our website anyway’.

The organisation tracks its threats and does regular security testing, with constant threat hunting exercises taking place. The CSO has identified eight different types of cyber security risk to the Board and says that processes are aligned to mitigating those risks and any chance of those sorts of breaches. In their words, ‘I would say before the breach I had 100% support of the Board and then post breach it was 110% support…. I would say this one helped accelerate the delivery of a lot of elements of my programme’.

Finally, the HSO also agrees that the organisation has ‘good controls in and good vulnerability management’. In their eyes securing talent is now the organisation’s biggest cyber security challenge as there is a dearth of candidates offering the right skills levels.

Case Study 4

Background

Private sector organisation in the construction sector with over 250 employees. Interviews conducted with the IT Director and Business Systems Technician.

In late 2019, the organisation was hit by a ransomware attack which affected its IT systems for two weeks. The unknown actor was able to access files on multiple servers.

Level of existing cyber security before the breach

According to the IT Director, there was relatively little understanding of cyber security at senior level within the organisation prior to the 2019 attack. Additionally, they noted that ‘the policies and process we had in place before [the attack] were robust but they were not policed strongly enough’.

The IT Director characterised the pre-breach cyber security setup as ‘adequate’ with ‘a plan in place to improve it’. Funds were already allocated for this plan to cover consultancy and technical investment. In their words, ‘I was really upset about the attack as we knew we had a weakness and unfortunately we just have not got round to addressing it’ due to other commitments taking priority.

Similarly, the Business Systems Technician noted that cyber security was not a ‘big concern’ for senior staff and ‘it is out of sight out of mind’. They regarded the organisation as reasonably secure because ‘I thought we are small fry so we are unlikely to attract a lot of attention, and I assumed our systems are locked down and up to the job’. Moreover, they trusted their third-party provider who is responsible for all their system development and upkeep. They did however reflect that in retrospect they had some ‘old hat systems and were probably quite vulnerable’.

The breach and the organisation’s immediate response

The organisation’s infrastructure is outsourced to a third party as part of a fully managed service. The attack happened at 3:00am and the IT Director was notified – in their eyes somewhat belatedly – approximately two hours later by which time the malware had started to close much of their network down, having branched out and accessed numerous files across its servers. In the words of the Business Systems Technician ‘it was not brought to our attention until things stopped working. We lost connections and then it snowballed and people across the organisation could not access folders or files and we suddenly realised everything is broken!’

The IT Director had a meeting with their outsourcers early that morning to ascertain the severity. This was followed by an emergency board meeting at 10:00am, by which time they had received emails from the unknown attackers demanding Bitcoin in return for a restoration of their systems.

The organisation had a policy in place to never pay ransom demands so the Board decided to instead do a ‘bare metal restore’ (‘a full business continuity restore’) to bring the system back to the state it was in before the attack. The IT Director was ‘really grateful’ to the Board for the rapid decision to proceed.

Two file servers and two PCs were affected but as the IT Director wanted to reduce the risk of others being infected, all head office computers were taken offline. As the organisation is ‘60/40 on the cloud’ some business units were not affected by the breach and suffered no loss of systems.

The IT Director reflected that he underestimated how long it would take to restore all the systems, as the process lasted two weeks and was ‘an irritant’. It did not however overly affect day-to-day business as employees had email and phone access, they simply could not access files on the server. Over this time, the Business Systems Technician felt that they played more of a ‘HR role’ than an IT role as ‘you are more of a support for people…trying to keep people happy and informed especially senior people. So, there was a lot of handholding and telling people what to do’.

The restoration plan was based on priorities, the first of which being to ‘get the operating system back quickly’. They deployed three different antivirus software tools before re-installing the operating system. Then they had to prioritise what data to restore, with ‘tier one data’ restored in six hours.

According to the Business Support Technician ‘the third-party incumbent responded quickly and they ensured everything was locked down and made sure the threat was not there anymore’. Over the two weeks ‘we had 15 to 20 virtual servers rebuilt and we re-scanned about 12 terabytes of company data in shared files before it was uploaded’.

Subsequently, there was a ‘forensic examination’ by the third-party provider to determine what exactly had happened. They identified that the malware had been sitting on the organisation’s system for around 18 months lying dormant. They were not however able to identify what triggered it to become active. Once it became live on a file server, according to the IT Director, it then ‘turned off certain security policies on the machine so allowing external access…. It was a very sophisticated attack, so we were very unlucky.’

Impacts upon the organisation

The breach had a ‘big impact’ on the IT Director emotionally. They offered their immediate resignation to the Board as they ‘could not keep the company secure’. The chairman declined their request and the Board ‘then encouraged me to put all the necessary security in place’.

The Business Support Technician also characterised the organisation’s leadership as ‘understanding’ and grateful for their hard work, although that started to change over the fortnight ‘as the business started to lose money’.

Subsequently the organisation invested around £10,000 on the forensic investigation along with penetration tests and tests of their additional security. They made no attempt to quantify other costs, such as loss of revenue, the time spent investigating and fixing the breach or the impact on employee productivity and customer relationships.

Furthermore, as no customer data was lost or downloaded the organisation did not inform any official bodies or its customers.

How cyber security arrangements have changed in the wake of a cyber breach

The IT Director reflected that ‘we are in a much better place now’. Previously the server access method was via an externally facing server and this was identified as the key security weakness. The malware turned off the password policy then launched a brute force attack, which after many thousands of attempts was able to crack the password.

Consequently, the organisation now has no externally facing servers and staff need to use Multi Factor Authentication (MFA) with three forms of authentication to access the system. They have also increased minimum password complexity.

In addition, the organisation has changed its firewall and the antivirus protection, and now uses different antivirus systems for servers and laptops / desktops.

Since the breach the organisation has put more emphasis on technology than people to stay cyber secure. Employees are though, according to the IT Director, ‘in many ways the weakest link so we have new ICT and cyber threat security training for individuals as well as a monthly communications bulletin and a twice-yearly security refresher’.

Their objective in the short to medium term is to have everything hosted as a service with Microsoft ‘with all the resilience that that brings…so if that data centre goes down it will not just be us, it will be thousands of companies affected’.

The IT Director stated that ‘I am very happy with it, we are in a much better place now especially with the focus now on education of staff and raising awareness’. The Business Support Technician also noted that ‘we have upgraded a lot, we are now on a par with if not ahead of the competition so in some ways we are reaping the benefits of the attack’. It has also prompted an improvement in service from their providers who are now doing ‘more scanning and monitoring and they are giving us more guidance and information and updates on security’.

Case Study 5

Background

A private sector organisation with under 10 employees. Interviews conducted with the Managing Director and Finance Director.

In January 2022, the organisation was hit by a DDoS attack which disrupted its internet and Voice over Internet Protocol (VoIP) services for three days.

Level of existing cyber security before the breach

Given the small size of the organisation, the Managing Director characterised themselves as being ‘responsible for everything’, including network management and servers and the IT infrastructure.

The Managing Director noted that, prior to the cyber attack, the organisation was better protected than the average company of a similar size. In their words, ‘in fact I work with companies ten times our size and their spend is nothing, they bury their head in the sand’.

Before the breach they were conscious of the threat of cyber attacks and were not ‘blasé about it’ as they ‘religiously followed firmware updates and software updates’. In addition, they had cyber security services from their internet service provider and had installed antivirus software on all laptops, desktops and phones.

The breach and the organisation’s immediate response

The organisation has experienced four attacks since 2018, each have been distributed DDoS attacks. The first three happened between August and November 2021, while the fourth and most impactful attack happened at 4:09pm on 21st January 2022. This was an attack on the organisation’s ‘core router’ which ‘jammed up’ its internet access and also ‘took out’ its VoIP internet telephones which are run by a third party.

At around 3:00pm, employees noticed that their systems were all ‘getting slower and slower, especially emails’. The Finance Director also found things to be uncharacteristically quiet with far fewer orders than normal from customers. The Managing Director was alerted to this and immediately rebooted their systems. Following this, ‘the internet came back as normal but then it slowed down again, and when I checked further it turned out that our inbound traffic was off the scale’.

The Managing Director contacted the internet service provider who informed them that their IP had been targeted by a DDoS attack. The internet service provider changed their IP address that afternoon, which was an ‘immediate solution’ to the attack. The Managing Director then had to reconfigure and change the organisation’s Domain Name System (DNS) settings. It took ‘72 hours for everything to be working properly, but over this period it was not the end of the world as we could access our mail servers as they are remotely sourced.’ It disrupted their VoIP as their IP address had changed; consequently, they experienced intermittent phone service over the three days.

Impacts upon the organisation

The Managing Director said it resulted in some lost sales but regarded it as too fleeting an attack to have a major financial impact on the organisation. In contrast the Financial Director was less sanguine and indicated that it did have a meaningful impact on revenue, although they were unable to estimate the scale.

The organisation also experienced negative customer feedback on their primary sales channels, mostly saying items had been delayed. The Finance Director was perturbed by this as ‘when it comes to eBay you have to proceed the same day with dispatching the products…but we had no access to computers so we could not follow the process, so we had a lot of complaints'. Consequently, their eBay rating suffered as 'we usually get five-star reviews, but it has gone down a bit as a result. It is very competitive and once you lose a customer it is unlikely they will come back to you'.

It was a 'challenging period' for the Finance Director that involved dealing with customer complaints while also worrying that they 'had done something wrong given my limited IT knowledge. I thought my knowledge was the issue.'

The Managing Director also found the experience 'highly stressful' as they did not know how long the attack would last. They did however reflect that in retrospect, 'it was a generic attack, we were not targeted. It could have been a lot worse'. It has, however, served to make the Managing Director and other employees more conscious of cyber security.

How cyber security arrangements have changed in the wake of a cyber breach

The organisation recently purchased a new firewall for £400 which 'amongst other things as soon as it gets bombarded will block out IP addresses'. The Managing Director has also imposed 'an unofficial policy' that all employees should go to them before opening any 'strange looking emails'.

Aside from this, the organisation has taken no further action as they do not have funds for further investment in cyber security training, hardware, or software. In the words of the Financial Director, 'when it comes to the technical setup, we are not a company that can spend thousands on it'.

Case Study 6

Background

Private sector wholesale and retail organisation with 50 - 249 employees. Interviews conducted with the CEO and IT Manager.

In November 2021, the organisation was hit by an attack which compromised its Microsoft Exchange server and used it to send out spear phishing emails to an unknown but large number of the organisation's contacts.

Level of existing cyber security before the breach

The IT Manager characterised the organisation as being 'in a good place' as 'we spent a lot of time and money on security over the last five years…. Compared to other organisations, I would say our approach is much more extreme and we are more secure'. The CEO also claimed they were 'ahead of the game' with 'robust' systems.

According to the IT Manager, the organisation operated various layers of security: hardware, internet gateway and switches were all 'state of the art security products'; there is also 'a lot of security on our servers'; and they spend around £9,000 annually on 'subscriptions from a world leading security firm'.

In addition, all staff were trained on data protection and GDPR, and they were coached not to click on suspicious emails, although beyond that there had been 'no specific cyber-awareness training'. Consequently, the IT Manager estimated that 'only 50 per cent of employees will recognise a strange email when they see one, but some will just click on it still'. This breach was not, however, due to the action of any staff member, as an external agent penetrated the organisation's security by exploiting a weakness in the software it was using.

The breach and the organisation's immediate response

The organisation became aware of the breach after people started to contact it in November 2021 to inform them that it was sending out 'strange emails'. It then took two to three days to isolate the problem. During this period, they stopped all outbound emails.

The external IT consultant that the organisation had previously utilised was unavailable at this time, so the IT Manager and their assistant dealt with the breach. They commented that 'we did not really feel that we were fully on top of it. It felt like a well-hidden panic.' And, although they stopped the initial attack, it recurred three times over the next fortnight as attackers circumvented the measures they put in place, 'however after the third attack we were confident nothing else was going out'.

Approximately two months after the breach, the organisation did confirm they had actually been infiltrated in March 2021, and 'something may have been dormant in our system' since then. It was discovered that a Microsoft patch was used as the vehicle for entry as it allowed a gateway to be opened by third parties. And, in the CEO's words, the investigation found that 'the virus was still rife across our systems and our software had not found it.'

Consequently, the IT Manager and their assistant set about getting 'clean' by 'rebuilding the IT infrastructure from scratch, servers, laptops, desktops and also moving the email from inhouse to remote.' Over this period, most of the data and applications that staff needed were available, 'but some of the niceties were not and that is why people were moaning'. By the time of interview in early March most of this rebuilding work had been completed, but employees still did not have access to old email histories or certain information. Most importantly, installation engineers did not have access to some online technical manuals and documentation which was a source of frustration for them.

According to the IT Manager, the attitude of senior management over this period was wholly supportive, as ‘it was to keep out of the way and let us do our job and there was no hesitation when it came to giving us more money’.

Impacts upon the organisation

The impact upon the IT Manager was considerable as they reported ‘working 16-hour days from November and right up until the last week.’ It took until early March for all ‘critical functionality’ to be restored, ending, in their words, the ‘initial phase of horror’.

The personal impact on the CEO has also been ‘significant’. They felt a great sense of responsibility as ‘I have a lot of staff who rely on us for their jobs…even now we still have weekly meetings on this issue.’

There was also a cost in terms of staff downtime and lost revenue that is ‘not easily identifiable’ according to the IT Manager. The CEO nonetheless believes that the breaches had a ‘huge impact’ on the organisation’s January turnover, not least because its email address (even when changing Top Level Domain) got barred by many client organisations. The CEO noted that one Local Authority Council banned its email domain so ‘the people in our business who run that contract cannot communicate with the council and we are still waiting to be whitelisted[1]…this sounds minor in terms of scope but it had a major impact on this account’.

There was also an impact on staff turnover with one experienced engineer leaving because they could no longer access the online documentation. Moreover, there was, according to the IT Manager, ‘a measurable upturn in stress, frustration and anger’ more generally amongst staff.

Furthermore, according to the CEO the direct cost is also ‘getting out of hand’ as ‘we have recently employed a new consultant in our IT department, we also have a new [Office] 365 license so we are already about £20,000 over and above what is budgeted for in our IT budget’.

While systems were compromised, it transpired that there had been no actual data breach or loss of data, the CEO felt that ‘our reputation and standing was really hammered and suddenly people were perceiving us as an unclean bunch who are not trustworthy, who will infect everyone who comes into contact with us.…So we are still in the process of trying to rebuild relationships and trust.…We have rebuilt our systems with new software but they still do not trust us’.

The CEO speculated that the organisation’s marketing and PR budget may need to increase significantly to support the ‘bridge building to be done with clients’.

How cyber security arrangements have changed in the wake of a cyber breach

One positive that has come out of the incident, from the point of view of the IT Manager, is that it has engendered a change in culture as ‘before I was the man who made it difficult to do things, which I think is standard, but now people understand what they are paying for’.

The most significant change to the organisation’s cyber security set up is that its Microsoft services are all cloud based; consequently, the IT Manager asserted that

[1] Respondent is referring to an ‘allow list’ - https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white

‘the major risk we are left with now is user risk as everything is managed off site by Microsoft’.

Case Study 7

Background

A very large private sector organisation with over 250 employees. Interviews conducted with the Chief Information Security Officer (CISO) and Head of Security Operation Centre (HSoC).

In the first quarter of 2021, this organisation was hit by a secondary attack when unknown actors impersonating it started sending out high volumes of smishing texts to its customers, directing them to fake websites.

Level of existing cyber security before the breach

This large and complex organisation employs over 150,000 people in the UK and, in the words of the CISO, views cyber security as a 'board level business problem as it involves financial risk, operational risk, strategic risk and customer risk.' The organisation is subject to high levels of regulatory scrutiny and control, and it is by nature very 'compliance focused' and 'technology focused'.

Consequently, the organisation has extensive cyber security technology and controls in place. It is constantly investing and upgrading as, according to the CISO, 'given the number of attacks and the type of attacks, the controls that were appropriate a few years ago are no longer appropriate now'. Moreover, as the organisation digitises and builds in more technology, its risk profile is growing and changing. This in turn 'requires a cultural transition so that employees become aware of these risks'.

Both the CISO and HSoC stressed that buying the technology controls is, in the words of the latter, 'the easy bit, it is the cultural change that is the challenge'. And, while leadership at the organisation 'get the idea that cyber is important', they do not yet fully understand 'the scale of it and the cultural transition the company needs to go through'. Middle management were deemed to be an even 'bigger problem' as many are long serving and now have to manage new technology. But the CISO also emphasised that 'we are in a good place, we have the budget, we have worked out the critical business processes.'

The HSoC is responsible for security event management and security incident response. In their team, two people look at incident response to events and three cover event management with support from a third-party supplier with 32 team members. The HSoC noted that they get 'an awful lot of events and our job is to contain or mediate them before they become costly or reputationally damaging….Certain things will generate an alert indicating that something malicious is occurring and that automatically starts a triage process. If this is validated, it becomes a security incident….We get about 72 incidents a week'.

A large minority of incidents are triggered by members of the workforce 'who are not that familiar with technology, so it is not all about cyber attacks'. This organisation has seen increases in cyber 'prodding and poking' attempts since the start of the COVID-19 pandemic, but according to the CISO 'we have protection in place against that, we have a very good service'. Moreover, the HSoC stressed that the organisation has had 'very few' successful attacks and they 'absolutely rely on technology and we have a lot of technology deployed across our estate', such as firewalls and advanced data protection tools.

The breach and the organisation's immediate response

Early 2021 saw a huge and 'unprecedented' increase in smishing attacks (A 'smishing' attack is a form of phishing in which the actor uses a compelling text message to trick targeted recipients into clicking a link and sending the actor information or downloading malicious programs to a smartphone). These attacks targeting this organisation's customers who 'were clicking on links in a text message that they thought were from us which were saying, for example, your parcel has been delayed.' The links would take customers to fake websites, often with the aim of tricking them into divulging confidential information. In order to appear legitimate, these websites had adopted the organisation's brand identity.

The organisation became aware of these attacks on customers 'early on' as the HSoC oversees a spam awareness process and provides an inbox for customers and employees to report spam SMS and emails. Their team monitors the inbox and saw a 'huge spike' during the pandemic.

To 'protect its reputation and of course to protect our customers who are subject to these attacks', the organisation took immediate action and has to date taken over 50,000 fake websites offline. It enlisted the help of a third-party provider to do this and also liaised with the National Cyber Security Centre as well as the NHS. Incidentally, the CISO has worked on combatting smishing in a previous role in the mobile sector so had significant experience dealing with these sorts of 'fake websites.'

According to the HSoC, in 2021 the organisation also 'stopped hundreds of thousands of SMS messages hitting customers by using tools that enabled us through the mobile ecosystem to gain early awareness of spam SMS messages'.

Impacts upon the organisation

Although the HSoC had a service in place to take down the fake websites, they noted that 'this process started to stretch my team further when we were already stretched as you are doing a lot more in the pandemic due to the increasing volumes of deliveries and changes in customer behaviour so it was more of a stretch for my teams…it has died down now, it was really more of an impact during the first half of the pandemic.'

But beyond the increased resourcing demands that were posed by this secondary attack there was little significant impact on the organisation.

How cyber security arrangements have changed in the wake of a cyber breach

For the HSoC, this episode was beneficial because it highlighted the importance of cyber security to leadership within the organisation as 'in the past the challenge for us is that we were partly a victim of our own success as we were so good at protection, we never had a major incident, so we never had evidence of the importance of cyber security'.

In response to the smishing attacks, the organisation has bought extra services to reduce the chance of secondary fraud happening to customers. It has also contracted external providers to identify imposter websites and work with the authorities to have them removed.

The CISO noted that they have also added content to their website to help people identify smishing and have increased communications on this issue to make customers more cyber-aware. In their words, 'we're becoming more proactive particularly using our customer touchpoints to show that we care and can help'.

Case Study 8

Background

Private sector organisation with 250+ employees. Interviews conducted with the IT Director and Finance Manager.

In December 2021, the organisation's CRM vendor was hit by a ransomware attack, which disabled its core CRM system.

Level of existing cyber security before the breach

With an annual turnover of over £150M the organisation invests 'about a quarter of a million a year on security' and in the words of the IT Director 'I would like to imagine that we take it more seriously than most other similar companies….I am stoic about it; I just want to be less attractive to actors than competitors.'

The IT Director leads a team of six and describes the organisation as well protected at the time of the breach with anti-virus software on all endpoints, a software solution for cloud security and a 'third party to look after this 24/7'. They also used cloud computing technologies and provided employee cyber security training and awareness raising. According to the Finance Manager 'we have security training videos at least once a month telling us to look out for things like phishing emails.'

The breach and the organisation's immediate response

The organisation had a supply chain breach in its vendor Customer Relationship Management (CRM) system in mid-December 2021. This recruitment CRM system is, according to the IT Director, 'the engine that runs the company as it has candidate details, booking details, pay rates and it is part of the process for making payments and pushing out information into our financial system'.

The supplier was rendered inoperable, so the organisation's CRM stopped working altogether. The breach itself was a ransomware attack on the vendor (who did not immediately notify the organisation). It impacted on a Saturday night and had propagated across the vendor's entire server estate by Sunday. This disabled their entire infrastructure.

The problem became apparent very quickly to the Finance Manager and their team on Monday morning as they were unable to verify their licences on the CRM system. Initially the organisation suspected it was an internal issue, so they undertook some immediate investigations. Over the course of that day the IT Director tried to get in touch with the vendor but could not get through to them, at which point they started to suspect it was a vendor issue.

Later that day they started to receive 'sporadic communications' from the vendor. In the words of the IT Director, 'it took about 72 hours for the vendor to tell us it was a basic ransomware attack as malware got into their server with admin credentials, so I guess someone on their side must have clicked on a phishing link.' It took the vendor 10 days in total to resolve the issue, which involved rebuilding the CRM system from scratch and backing up the infrastructure. The organisation however was able to get its licensing server back up and running after two days which crucially allowed it to re-start some of its key business processes.

As the Finance Manager noted, 'we host everything on our internal platform, it is just the licensing that is held on their environment. So, once they resolved the licensing issue we were okay'. Nonetheless, it was a 'very awkward period' with 'all hands-on deck shoring up the business'.

Impacts upon the organisation

Most employees could not use the organisation's CRM system for two days; some physical machines were operable but ‘we had to scramble around to get these machines to the right people.’

This was ‘hugely disruptive’ to the organisation as it is ‘very important’ that certain business payments are made daily, otherwise ‘you are in trouble’. According to the Finance Manager, their team were ‘flat out’ for at least a week managing the fall out of the delays. Similarly, employees in sales and customer service roles did not have access to key information. Consequently, there was also an impact on the volume of sales made over that period.

Therefore, while the overall cost of the breach on the organisation has not been quantified, the finance manager was confident it is ‘tens of thousands of pounds’.

The organisation decided not to formally notify customers, the Information Commissioner’s Office (ICO) or other official bodies of the attack as it did not constitute a personal data breach.

How cyber security arrangements have changed in the wake of a cyber breach

The IT Director reflected that the supplier attack was good, focusing the minds of senior management on cyber security and for ‘getting the business to invest on the security side of things [as] they have given me everything I need since then’. This includes a new ‘managed service with agents on all devices and monitoring on our Microsoft environments’ as well as Phishing Tackle software which sends simulated phishing emails to help train staff and identify weak spots.

Going forward, the IT Director will put more of an emphasis on technology than people when it comes to cyber security ‘as I think we need to get humans out of the picture but keep them as aware as possible and help them to be careful’. They therefore contracted a vendor to provide automated phishing simulations to help train staff to recognise potential attacks and to identify who are most click-prone. The organisation has also recently introduced a ‘sandbox’ which ‘looks at emails and stops people being able to open questionable emails’.

In addition, they are working on a vendor risk assessment process to better understand how their vendor secures and monitors the environment, and their notification processes in the event of a breach. The organisation is also changing its backup suppliers and is working on a disaster recovery site as part of an ongoing business continuity project.

Case Study 9

Background

Private sector organisation with 10 - 49 employees. Interviews conducted with the Head of Strategy and IT & Risk Manager.

In March 2020, the organisation was hit by a ransomware attack. Using a Trojan, the unknown actor was able to gain access to and encrypt the organisation's IT systems.

Level of existing cyber security before the breach

Both participants perceived their senior management to be 'supportive of cyber security' and 'happy to invest'. In the words of the Head of Strategy, 'I think we did everything reasonable that you could expect from an organisation of our size when it comes to staying secure'. The IT & Risk Manager, however, described security as 'adequate' but not 'all singing all dancing'.

Prior to the breach, the organisation had firewalls in place, antivirus software and two 'new' servers. The organisation had also invested 'tens of thousands' in a 'box in our offices that saves data to the cloud continuously' (required because they hold insurance data).

They used an external provider, who offered 10 days per month of IT support 'that covers crisis and also the day-to-day stuff'. In addition, the provider delivered online training every six months to employees and it also 'targets members of staff at random to see who will click on dodgy links.'

The organisation had an informal process in place whereby suspicious emails were sent to the provider for screening. And whilst it did not have a formal cyber security policy, its IT usage policy provided guidelines, for example not to access non-business-related websites, or not to use USB ports.

The breach and the organisation's immediate response

The business faced two similar attacks in quick succession. Both were 'Trojan attacks' in the shape of emails from a recognised client with an attachment that appeared legitimate. In each instance, clicking on the attachment led to a ransomware attack.

The first attack was the most impactful – and could have potentially led to the greatest harm – as it targeted the Managing Director of the organisation who is responsible for many of its largest accounts. Upon opening the attachment, a padlock appeared on their screen, after which 'the firewall kicked us all out of the system'.

As a result, employees were aware of the breach almost immediately, as they were all working from home due to the pandemic and the Virtual Private Network (VPN) cut off 'so the system disappeared for everyone. Our screens were blank'.

The IT & Risk Manager contacted the external provider straightaway. They advised that the organisation needed to close all computers immediately to limit the spread. The IT & Risk Manager also sent out a text message to all employees informing them of the virus and not to access the system.

The IT & Risk Manager spent the rest of the day liaising with the external provider and with the directors and the rest of the staff. The provider came in that morning to investigate the problem and to ensure there were no 'Trojans in the system that will reappear'. By the evening they were ready to reboot the system to a pre-breach position. According to the IT & Risk Manager, 'as we did not know when the attack had happened, we rebooted the system back a few hours…this was at about

9:00pm'.

The external provider reset passwords for all of the staff the next morning and helped them get them back onto the system 'which also took a few hours'. They then conducted further checks to assess if any data was lost. They concluded that this had not happened, and nothing was compromised. Consequently, the organisation did not have to inform any external parties of the breach.

Impacts upon the organisation

The Managing Director who clicked on the malicious link felt 'sick with the stress of it' according to the Head of Strategy, 'particularly as we were just going into lockdown and coming to the end of our financial year, so it was terrible timing… [they are] now much more wary of IT issues.'

For the IT & Risk Manager, 'the first few minutes were stressful, but I had confidence in [the vendor] and so once they were involved it was reassuring'. Similarly, the Head of Strategy 'was not too anxious' about data back-up and recovery but was initially concerned that sensitive personal data on the Managing Director's PC could have been compromised.

The organisation has not undertaken a formal lesson-learned exercise or quantified the cost of the breach, but both participants estimated that the full cost to the business was in the range of £10,000 to £20,000 due to lost productivity and income in the downtime and in additional charges from their external provider.

How cyber security arrangements have changed in the wake of a cyber breach

The Head of Strategy noted that since the breach that they are always 'slightly on edge' but 'as we have been through it, we are more knowledgeable now as a team as are our staff…I feel reasonably confident about the future.' They also mentioned that they have shared their experience with some clients to highlight that they need to have cyber security insurance cover for their organisations.

Since the breach, the organisation has commenced a weekly training session for staff which 'helps to keep your eye on the game for phishing, vishing and so forth…. It is a 5-minute read and then you have to answer 10 questions and you need to get 80 per cent to pass.'

The organisation has also strengthened its security by 'increasing the settings on our antivirus software' and changing its email settings in Outlook so that it includes a quarantined email section as well as a junk mail folder. It is also planning to obtain Cyber Essentials accreditation.

Case Study 10

Background

Private organisation with over 250 employees. Interviews conducted with the IT Director and IT Manager.

In January 2022, an unknown actor was able to access this organisation's email account and use it to send out a high volume of phishing emails.

Level of existing cyber security before the breach

The IT Director characterised the organisation as 'immature' when it comes to security as 'we are in the education sector and from what I have seen it is not particularly cyber aware even though it is very GDPR aware.'

The IT Director was hired by the organisation to address this challenge, not least because the strength of its cyber setup was variable across its estate, and this was partly a product of there being no single ownership of cyber security. The pandemic did also adversely affect the organisation's revenue which has slowed the rollout of the IT Director's planned cyber security improvement programme.

Nonetheless, by the time of the attack in January 2022, everything was 'out in the cloud and run for us by third parties. That covers things like our procurement and finance systems, so I am confident they are sat behind good firewalls.' The organisation had also recently invested in a new firewall for its internal server.

The breach and the organisation's immediate response

The one successful breach had only limited impact. The organisation uses Amazon SES (Simple Email Service) to send emails out to the bulk of its customers, typically for invoicing and general communications. An unknown actor was able to steal the login credentials of that service and then used it to send a high volume of spam emails to 'random people.'

Amazon spotted the breach as they had controls in place that flagged it and they alerted the organisation to the issue. Upon receiving this news, the IT team immediately logged onto their console and saw that a 'huge number of spam emails had been sent'. Their first task was therefore to evaluate what had been sent. In the words of the IT Director, 'we could see that there were no spoof emails to our clients, they were just general phishing emails'.

The IT Team then went through a process with Amazon to suspend the account so no more emails could go out, while also cleaning and deleting email queues. After this, 'Amazon slapped our wrists, then we changed our password and Amazon reactivated the account'.

Once the system was restored the IT Team conducted a review of what happened and how it happened. The IT Manager – who has a background as a web developer – was quickly able to ascertain how the unknown actor obtained passwords for their Amazon SES account. The vulnerability was on the organisation's website which is 'deployed using standard tools (WordPress) and it generates files and they are publicly visible'. The unknown actor used tools to look for vulnerabilities and saw that embedded in the deployment files on the site were details of the organisation's Amazon account and password. Incidentally, the organisation had a penetration test around a month before the breach and it had not found this vulnerability.

The IT Manager immediately eliminated that vulnerability – 'I cleaned it up and updated our credentials so the password is different, and they could not log in anymore.' They then double checked all the organisation's other websites to ensure there were no similar weaknesses.

During the period of the breach, while the IT Manager resolved the issue and revised associated vulnerabilities, the IT Director took the 'business communications role' keeping the Board updated and documenting the process as it evolved.

The organisation did not need to communicate the incident externally as there was no data loss or data breach, although according to the IT Manager 'we sent an email out to clients saying we had a vulnerability, but it was now fixed and to ignore any spam emails from us.'

Impacts upon the organisation

The IT Director estimated that the breach cost them at most two days of staff time. They noted that the financial impact was also limited, partly because of the timing. 'It happened at the end of January, if it had happened just a little bit later in early February when we send invoices out…it could have delayed our cash flow.'

How cyber security arrangements have changed in the wake of a cyber breach

For the IT Director the incident was beneficial as 'it helped us and the wider IT team and leadership see that these issues are real so it sharpened up their thinking. There was a general sense across the business that no one is interested in us as we are below the radar and only small but…it has really sharpened up their awareness.'

Since the incident, the organisation has increased the size of its learning and development team so that they can deliver more cyber training and they are also pushing more information on cyber security via the Intranet and email. In addition, it has moved each of its websites onto their own 'separate virtual machines' so that they are isolated.

Laptops and how they are used are now the IT Director's main cyber security concern as there is 'a lot more to do on the desktop and end user environment and we are working with an external supplier on this.' Similarly, the IT Manager stated that 'I am trying to push a big roll out of two factor authentication.'

The organisation is also working towards Cyber Essentials accreditation.

6 Report writers and contributors

- Alec Folwell, Ipsos
- Tom Cox, Ipsos
- Yasmine Lamb, Ipsos
- Professor Steven Furnell, University of Nottingham

7 Appendices

DCMS - Cyber
security breaches - T

8 Our standards and accreditations

Ipsos' standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.

ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos MORI was the first company in the world to gain this accreditation.

Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos MORI endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.

ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.

ISO 27001

This is the international standard for information security, designed to ensure the selection of adequate and proportionate security controls. Ipsos MORI was the first research company in the UK to be awarded this in August 2008.

The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018

Ipsos is required to comply with GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.

HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos MORI was assessment-validated for Cyber Essentials certification in 2016. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.

Fair Data

Ipsos is signed up as a "Fair Data" company, agreeing to adhere to 10 core principles. The principles support and complement other standards such as ISOs, and the requirements of Data Protection legislation.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

https://www.ipsos.com/en-uk

https://twitter.com/IpsosUK

About Ipsos

Ipsos works closely with national governments, local public services and the not for-profit sector. Its c.200 research staff focus onpublic service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.