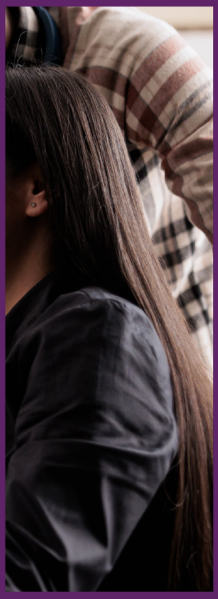
TSG
TECHNOLOGY SERVICES GROUP

Microsoft
Solutions Partner

Prevention versus cure:

Are businesses prepared to fight cyber-attacks?



Contents

As the world of tech continues to innovate and businesses increasingly turn to cloud-based solutions and AI to drive processes, IT infrastructure and data are becoming increasingly exposed to the risk of impending cyber-attacks.

According to a study carried out by Verzion in 2022 - despite business investment into cyber security, ransomware attacks continued to rise by 13% that year. This indicated a significant increase that overshadows the last five years combined. From just this stat alone, we can conclude that not enough was being done last year to protect our data. It's a problem that continues to persist, as a more recent study carried out in 2023 by Zippia found that a cyber-attack currently happens every 39 seconds, with 43% targeted at small businesses.

With this in mind, TSG commissioned Atomik Research, an independent creative market research agency, to:

- Understand the current state of play of SMEs within the UK market.
- Identify underlying issues that are leaving businesses without the correct processes to defend their data.
- Offer guidance on how to prevent future attacks and highlight how an experienced security-focused IT partner can support them long-term.

The research fieldwork was conducted from the 14th to the 16th March 2023, generating 151 responses from the UK's IT sector at DM, director level, or above.

The juxtaposition of cyber security

85% of businesses that we spoke to admitted that cybercrime was a concern, or very big concern, for their business - something that is reflected in PwC's global digital trust report. This report cites that two thirds of executives consider cybercrime as their most significant threat in the coming year. Despite these telling stats, companies simply don't always have the processes in place to protect themselves from a potential breach, with 60% admitting that they don't have security audits or threat assessments in place.

In the survey, business data was voted the most valuable (18%) and most vulnerable (22%). These contrasting stats stress the concern of the market, as the majority of businesses are struggling to protect an asset they consider to be their most valuable one.

Common cyber threats to your organisation include hacking, phishing, malicious software and distributed denial of service attacks against websites – all of which could have a devastating effect on a business. Therefore, it's imperative to cover all bases when implementing cyber security.

85%

of businesses that we spoke to admitted that cybercrime was a concern, or very big concern, for their business

To offer an idea of the appropriate levels of security needed, businesses should:

- Be regularly scanning for vulnerabilities, identifying weaknesses and implementing posture reviews
- Invest in strengthening their top cyber weaknesses
- Regularly commit to trend analysis and risk reduction reports
- Implement disaster recovery and external penetration testing
- Provide user awareness training
- Have a managed detection and response plan in place

Small changes for stronger protection

When it comes to protecting data, we all know about the technical measures that we need to put in place. However, often the simplest actions can have the biggest impact.

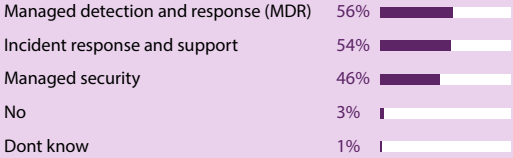
Claire Vandenbroecke, Cyber Security Specialist at TSG, lists some of the more common mistakes that she sees businesses making every day:

1. Assuming attacks will never happen to them
2. Not checking haveibeenpwned.com to see if your email address, password or mobile phone number has been leaked in a breach (you can sign up for alerts to save you checking each day)
3. Leaving your work or personal devices unlocked or unattended in public
4. Talking loudly about work in a public environment such as on a train or in a café
5. Sharing personally identifiable information about yourself or your business on social media, such as photos which reveal sensitive information in the background or geolocation tagged posts, which could be used by a criminal to commit fraud or send phishing emails to your friends, family or colleagues

Cyber security is constantly evolving and although 82% of businesses said they would know what to do in the event of a potential breach, over half of businesses fail to have managed security in place. In addition, 46% don't have an incident response and support procedure, and 44% do not have managed support and detection, suggesting businesses are not up to date or aware of the security processes needed to detect and recover from an attack.

Would you know what to do if your business suffered a potential breach?

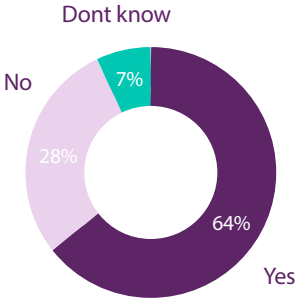
Does your business have any of the following in place



Although businesses are certain that they can respond to a breach, the survey reflects key areas where they could be effectively preventing their chance of an attack. Since 88% of data breaches are caused by an employee mistake, staff training is a huge opportunity to prevent a breach.

However, half of businesses admitted that this fundamental part of cyber security has not been actioned in the last six months. This stat grows in concern when considering that 64% of businesses reported that their staff use personal devices for work, increasing the need for regular training.

Do your staff use personal devices for work purposes?



> Businesses often lack the necessary resources and expertise to develop an effective security plan, which would help them achieve easy wins, such as staff training and implementing a Joiners, Movers, Leavers (JML) policy. Both of these actions could prevent a number of attacks.

Claire Vandenbroecke
TSG Cyber Security Specialist

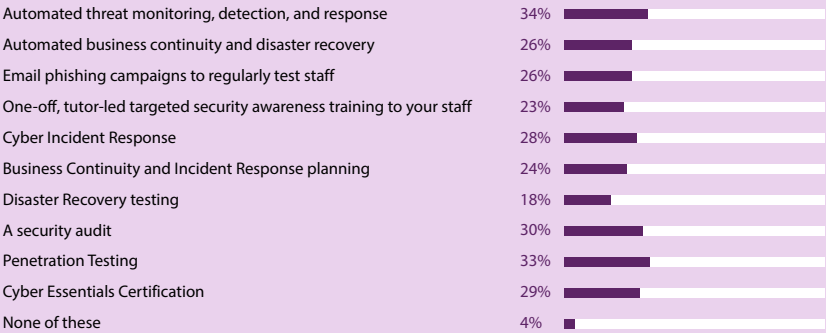
The importance of investing in prevention

Although it's important to have a contingency plan and incident response in place, these should be the last line of a business' defence. The best way to protect against cyber-attacks is through initial prevention.

In a world where cyber threats are constantly evolving, prevention techniques help businesses to keep their processes and teams up to date, so they can stay ahead of curve and protect against cyber-attacks. Although to cover all bases, prevention can take a lot of initial resource or cost, reacting to and recovering from an attack will cost a business a lot more, such as the loss of customers and reputation.

When asked what a business anticipates bringing into their cyber security plan in the next 5 years, 34% of businesses said automated threat monitoring, detection and response on their business network, which was followed by security auditing (30%), penetration testing (33%) and phishing campaigns to regularly test staff (26%). Our research data suggests that companies are aware that prevention is needed, however since they don't have the resource to commit to prevention across all areas, they are scrambling to ensure they can at least detect and respond to an attack to keep their business afloat.

What do you anticipate bringing into your business in the next 5 years?



A key area that businesses overlook and one of the biggest back doors into a company is through a third-party supply chain. This occurs when an attacker infiltrates a business' system and gains access to their data through an external partner.

According to Sonatype's 8th Annual 'State of Software Supply Chain' report, the average annual increase of software supply chain attacks has increased 742% over the past three years. Alarmingly, one in four companies surveyed don't have a minimum security-standard in place for third parties, leaving them vulnerable to an attack at any time. Ideally, they should have security standards in place that all third-parties abide to, and be working with organisations that have accreditations such as, Cyber Essentials or ISO9001.

Without any third-party precautions in place, whether companies are investing in prevention or reactivity, they are doing so inefficiently, as attackers will be able to take multiple routes into the business, time and time again. And it's not something businesses are taking lightly. According to PwC's report outlined earlier, over half of CRO and COOs are extremely or very concerned about their company's ability to withstand supply chain attacks.

The effects of failing to protect a business can vary and depend on the quality and level of cyber protection a company has in place.

From electrical blackouts and software paralysis to the theft of sensitive customer or business data, a cyber-attack can lead to the downfall of a company. A demise in reputation could lead to the loss of customers or even third-party suppliers or partners. Moreover, attackers could hold information or systems hostage and blackmail users into sending a lump sum of money.

Overall, without the correct systems in place, an attack will lead to loss of revenue and could completely close a business depending on the scale of the situation.

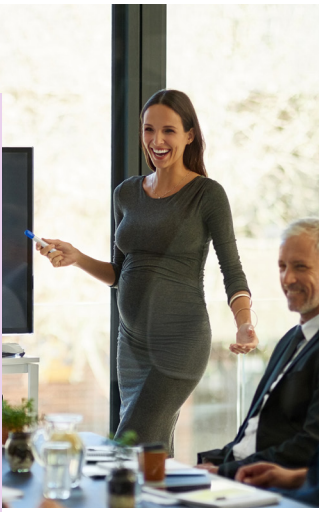
Overcoming the barriers to a secure infrastructure

So, if businesses are aware of cyber attacks and that their data is vulnerable, why are they not investing in the security to protect it?

Board buy-in, resource and time made up 74% of answers around the biggest blockers to implementing security in our survey, with almost one third stating that board buy-in was the top blocker to cyber security.

What would you consider to be your biggest blocker to implementing cyber security?

Board buy-in	30%
Time	24%
Resource	20%
Budget	19%
Knowing where to start	4%
Knowing who to trust	3%



Lack of board buy-in

Getting the board involved in a long-term investment is always difficult, especially when it isn't showing effective returns. They don't want to look at the 'what if' and infuriatingly opt for phrases like 'we will cross that bridge when we come to it'. Like our survey, other reports have reflected similar blockers. PwC's report states that 59% of their directors say that their board is not effective at understanding the drivers and impacts of cyber risks on their organisation. Meanwhile, in IPSOS' report on 'Exploring Organisational Experiences of Cyber Security Breaches', interviewees share examples of how their security posture strengthened following an attack, once senior managers realised the importance of investing in IT cyber security.

Does this mean companies will only act in the form of investment once they've realised the seriousness of cyber security?

IT leaders need to be putting together a full-proof report to the board, with alarming stats and examples that demonstrate the devastating effect an attack could have on the business. Another way could be to present the worst-case scenarios and offer figures that show the likelihood of this happening. Only then may they start to listen.

Resource and time

Even with the board buy-in, a full IT team would struggle with the experience and time to implement a full-proof cyber security plan. That's why investing in an IT security partner, like our team at TSG, is an effective idea. With years of experience and partnered with Microsoft, we're able to deliver tailored cybersecurity that can identify a business' vulnerabilities and work with them to strengthen their cyber defence.

Not only are businesses investing in experience with an IT partner, but they're also investing in the automations and tools that we're able to implement, as well as the knowledge and network that can future-proof defences by ensuring that our clients are always ahead of any new attack methods or opportunities.

One of our specialists, Claire Vandenbroecke, recently spoke on how AI can be used to prevent cyber-attacks

AI can be used to support IT security technicians in their day-to-day cyber security operations. AI can filter through vast amounts of data in real-time, much quicker than a human being can, and it learns as it goes, meaning it can better identify anomalies, potential weak spots in security and false positives in reporting tools.

Human error is a major contributing cause in security breaches, so providing existing IT security technicians with AI tools to support them in safeguarding their company network against cyber-attacks can reduce the burden on staff, leading to an increase in productivity and better working conditions.

Hackers do not keep regular business hours and will be conducting their attacks from different time zones. AI can protect businesses' sensitive data 24/7 without tiring, identifying threats as they occur and not putting them off until the start of the next working day when it may be too late.

The future of IT security in business

Cyber attackers don't discriminate and will come after large and small corporations. As we head into the future, businesses need to build resilience against the attacks, as failing to detect and prevent malicious breaches will only lead to repeat offences.

It's encouraging to see that a priority for businesses in the next five years is implementing automated threat monitoring, detection and response, which will cover businesses through from prevention to reaction. The blanket cover of protection may be the reason that it is a businesses' priority to implement, however businesses did value systems like penetration testing, as well as business continuity and disaster recovery over it.

Penetration testing was considered the most valuable to businesses. Its ability to stress test a business' security posture makes it an incredibly useful feature to have, however it lacks value if a business doesn't have the systems and processes in place to act on what it discovers.

The lack of correlation between what is valued by a business and what they are anticipating to implement in the next five years suggests that there could be lack of knowledge, skills and resource to deliver an effective security plan. With an IT security team in place, the correlation of system value and priority of implementation would be closer aligned in comparison, as we'd be able to diagnose the weak points of the business and create a prioritised plan that would deliver the most value.

Although board buy-in does need improvement, as we head into the future, we only anticipate this will increase. According to PwC's Global Digital Trust report, 51% of CEOs and board members are already demanding cyber risk management plans for major businesses or operational changes. This will only rise as more companies are educated and experience the backlash of an attack.

51%

of CEOs and board members are already demanding cyber risk management plans for major businesses or operational changes

Report summary

Whether through an attack on their own business or others, businesses are slowly waking up to the importance of cyber security, however they aren't implementing or adapting their security plan quick enough to prevent attacks from business back doors such as the third-party supply chain, leading to the significant rise in successful cyber-attacks. The majority of businesses that are yet to implement cyber security processes, they're struggling due to key blockers, such as board buy-in and resource.

Without action, the figures are only going to increase, leaving businesses vulnerable and leading to a lack of mistrust around IT infrastructure and processes. As the cases grow, businesses will continue to panic and scramble to build a final line of defence, throwing their efforts at a contingency plan.

However, to actually combat the growing concern of cyber security, businesses need to build a solid business case to take to their board of directors, demanding an investment in the prevention of security breaches, which will only help their credibility with other third-party partners and build resilience against the potential of an attack.

To make this a possibility, businesses need to be looking to IT partners for support.

At TSG, not only do we have the knowledge and data from insight reports like this to build a business case to take to a board of directors, but we have the time and resource in-house to diagnose the issues within the business and implement a security plan that's tailored to a business' issues. What's more, we have a vast network and work with partners such as Microsoft, allowing us to offer the best security products in the market.

TSG
TECHNOLOGY SERVICES GROUP

Microsoft
Solutions Partner

Ready to take your cyber security to the next level?

Get in touch

Email: info@tsg.com
Website: www.tsg.com

Prevention versus cure:

Are businesses prepared to fight cyber-attacks?