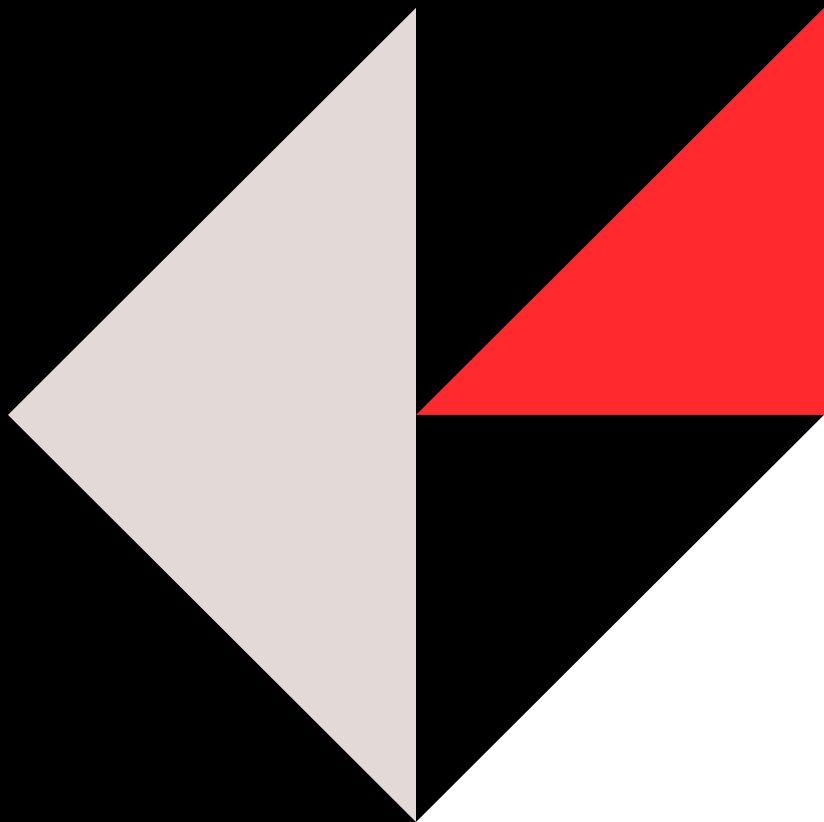
Global Security Research Report

The race to adapt

How your cybersecurity posture is affecting your business' bottom line



fastly

Table of Contents

Executive Summary

The past twelve months have been marked by continued global conflicts, financial instability and technological developments. These have all combined to create a feverish business environment characterized by high customer turnover, fiscal challenges and declining profits. Cybersecurity plays a major role in keeping a business' operations online, and the negative impacts from a security breach go far beyond mere system downtime. This report explores the long-term effects of cyber breaches, their effects on businesses, and how businesses can optimize their cybersecurity strategies to protect themselves from future attacks.

To better understand the challenges these organizations face and the drivers, developments and trends that are influencing their cybersecurity strategies, Fastly together with Sapio, a leading professional business and consumer market research company, conducted a global research survey of 1,484 key IT decision makers in large organizations spanning multiple industries across North America, Europe, Asia-Pacific and Japan.

Our findings revealed the major scale of cyber attacks, and the long-term damage they cause to businesses in both customer trust and loyalty, and how this negatively affects these businesses' revenue. They also showed the extent complexity continues to dictate cybersecurity strategies, one year on from our 2022 report: *Fighting fire with fire: Cybersecurity strategies are suffering as a result of complexity*, which demonstrated the harmful effects of relying on too many security tools. Additionally, our data uncovered significant reasons for optimism in the security industry. Particularly notable is the emergence of Generative AI technology, which security professionals are already adopting to reduce their workloads, and offer solutions to the shortage of emerging talent.

The results highlight the key priorities that will dictate organizations' cybersecurity policies in 2024:

- **Cyber attacks are highly varied in scope and type, but all can cause major damage, which seriously affects businesses' bottom lines.** The businesses we surveyed have lost an average of 9% of their revenue in the last 12 months as a direct result of cyber attacks. The most common threats businesses are grappling with are ransomware attacks (29%), closely followed by large-scale DDoS attacks (28%) and open source software vulnerabilities (25%), which demonstrates the range of threats businesses need to secure themselves against.
- **Cybersecurity footprints are becoming increasingly complex and businesses need to counteract this to avoid spiralling costs.** Cybersecurity budgets continue to rise with three quarters of businesses (76%) targeting an increase to their cybersecurity spending in the next 12 months. But, as security increasingly becomes a moving target, how can organizations secure themselves without continuously escalating spending?
- **Generative AI is not to be feared. It is a useful tool to reduce toil and help to solve many of the challenges the cybersecurity industry faces, particularly with the talent pool.** While 35% of cybersecurity professionals predict Generative AI will be a major threat driver in the next year, 77% estimate its impact will be positive in the long term. Above all, businesses are recognising the potential Generative AI offers in reducing toil for overworked security teams, and seeing it as a solution for ongoing challenges with recruiting suitable talent.

The unexpected damage caused by cyber attacks - and how long it takes businesses to recover

It will come as no surprise to anyone who reads the news that cybersecurity breaches are highly damaging. IBM estimates that the average cost of damage caused by cyber attacks has increased 15% over the last three years. Our own data also demonstrates exactly how significant the negative results of cyber breaches can be, and proves why cybersecurity must be a priority for businesses now and in the future.

Over the past twelve months, the damage caused by cyber attacks has been staggering, with the businesses we surveyed reporting an average revenue loss of 9% resulting directly from cyber attacks. The worst hit region in this respect is the UK, where businesses have lost over a tenth (11%) of their revenue as a direct outcome of cyber attacks. This represents a major loss for businesses who are already suffering under an extremely challenging economic climate - and a significant imperative to rethink security spending to improve its effectiveness.

In a world where nearly all (93%) of businesses surveyed are currently operating in a fully remote or hybrid structure and the vast majority of these (78%) believe remote workers are harder to secure than in-office employees, a crucial piece of the cybersecurity puzzle is education. Indeed, only 16% of the security professionals we surveyed truly understand that on-site and remote workers require the same security controls to keep them secure when security is properly implemented.

All of this poses the question: what does a truly effective cybersecurity strategy look like?

First of all, we need to take a step back and assess what the threat landscape looks like in 2023, and how it has evolved - and will continue to evolve - over the past year, and in future. To understand this, there are several factors we can examine. The principal concern of many security teams will be the kinds of threats they have to protect their organization against. Over the past year, the most common attacks suffered by businesses have been: Ransomware (29%), DDoS (28%), Exploitation of vulnerabilities in open source software (25%), Social engineering (22%), API/web application-related attacks (20%) *(Figure 1)*.

Figure 1

Most common attacks

1	29%	Ransomware
2	28%	DDoS
3	25%	Exploitation of vulnerabilities in open source software
4	22%	Social engineering
5	20%	API/web application-related attacks

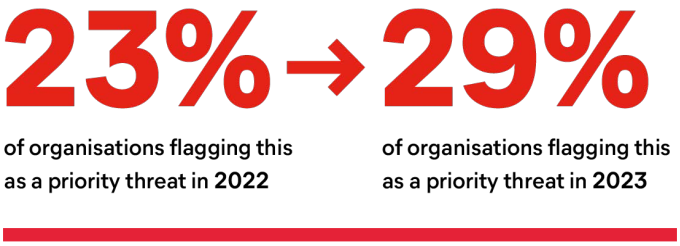
Particularly alarming is the extent to which social engineering attacks - including ransomware - are an increasing avenue for bad actors to gain access to organizations, with 29% of organizations flagging this as a priority threat, compared to 23% in 2022. Their frequency only serves to reinforce the clear need for businesses to implement effective cybersecurity training plans across their entire team, to ensure they are able to recognize the telltale signs of a social engineering threat and mitigate its damage.

The ongoing exploitation of open source software is an additional area of significant concern. This is because the entire supply chain is targeted in these instances, meaning every programme that is developed will have the same vulnerabilities. This commonality ensures open source software will always be a target for bad actors.

Sean Leach, VP Technology at Fastly, explains how a secure-by-design mentality can protect programmes built using open source software, *'We were founded by developers and, as a result, giving back to the open source community is extremely important to us. As a result, we are proud of our support of open source initiatives, and of the atmosphere we have fostered for these to thrive through our Fast Forward programme. We have fostered this ecosystem with a secure-by-design mentality, ensuring that security is the default for any developers using our technology, and closing a significant avenue that bad actors can exploit in other open source networks.'*

It's also vitally important to consider the scale of the threat that faces businesses operating in today's landscape. Worldwide, businesses have suffered an average of 46 known cyber attacks in the last twelve months - equivalent to almost one per week. The frequency and severity of these attacks poses a significant danger to organizations, while also forcing security teams to be on high alert at almost all times.

Figure 2
Social engineering attacks (including ransomware)

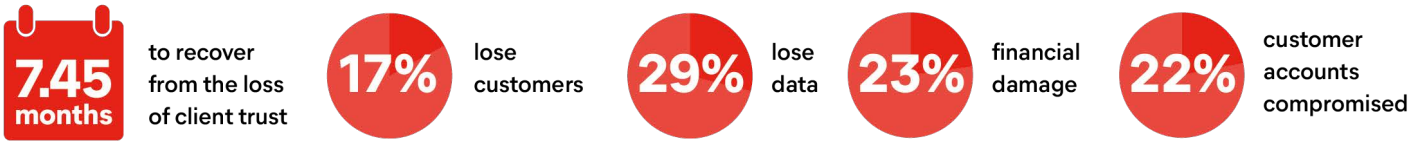


Indeed, over the past year, cybersecurity professionals estimate that the drivers of the most significant threats are highly diverse and encompass both external and internal factors. These range from the complexity of the threat landscape (35%) to attacks on remote workers (33%), and a lack of internal education on cybersecurity best practices (32%). Despite the severity of each of these driving factors, their scale does not match the predictions made by cybersecurity professionals in 2022, when concerns around remote workers topped our ranking (46%), closely followed by the increasingly complex threat landscape (40%) and a lack of internal education on cybersecurity best practices (39%).

One major cause of this disparity is the rise of Generative AI (32%), which has recently been a major source of concern for security teams, and carries with it significant implications for security teams. Indeed, security professionals predict the challenges caused by the emergence of Generative AI will only continue to grow, with over a third (35%) predicting it will be a major threat driver in the next year.

Regardless of their cause, it is the effects of cyber breaches that really hit businesses where it hurts. While every piece of damage caused by a cyber attack has a direct negative effect on the target organization, each of these also causes a chain reaction as customers and clients are affected. This, in turn, causes longer-term damage to the business as future customer relationships are jeopardized, resulting in long-term revenue losses.

Figure 3
The effects of cyber breaches on business



On average, it will take businesses 7.45 months to recover from the loss of client trust as a result of a cyber attack. That's a long time, and is highly sobering for organizations which cannot afford to lose out on nearly 8 months of business. Additionally, once trust is broken, it's very difficult to recover. This means a single cyber attack - particularly one resulting in a customer data breach - will have long-term impacts on the business that suffers it. During an uncertain economy, this revenue hit can risk a business' future viability.

The other effects of cybersecurity breaches are no less damaging and can affect an organization's critical operations. Nearly a fifth of breaches (17%) directly cause the affected business to lose customers, while nearly a third (29%) lead to data being lost. Additionally, negative financial ramifications of security breaches are highly common, with 23% of attacks leading to financial damage, and 22% resulting in customer accounts being compromised *(Figure 3)*.

These results demonstrate the direct impacts of cyber attacks, showing exactly why it is vital for businesses to shore up their cybersecurity posture for their protection, but also to ensure their clients' security. It is vital to emphasize that cyber threats do not just affect your business, but also the customers and clients that make your business run. For this reason, having an effective cybersecurity strategy is no longer simply an operational necessity, but also a business imperative.

How to hit the moving target of cybersecurity - Is spending spiralling out of control?

With an effective cybersecurity strategy becoming an increasingly important part of business operations, it is vital for security teams to work within a framework of profitability, and prove their value. With security threats being as diverse as they are, and the desired outcomes of an effective security strategy becoming increasingly scattered - especially as businesses try to protect themselves from individual threats - it can be easy for security spending to spiral out of control.

The result of this skyrocketing spend is that businesses are more consciously considering how they allocate cybersecurity budgets, assessing their budgets against risk. Opinion is divided over what effective security spending looks like: over a third (35%) feel they overspent in the last 12 months, compared to a fifth (19%) who feel their spend was inadequate. One near constant, however, is that cybersecurity spending will continue to rise, with three quarters (76%) stating they will increase cybersecurity spending in the next 12 months. This also marks a slight increase year-on-year, with 73% anticipating increased security spending in 2022 *(Figure 4)*.

A constant theme throughout the findings of our survey has been the security challenge many businesses are facing as a result of shortages in the talent pool. The fight for the right talent has become increasingly competitive, and is one area where many businesses (48%) are having to increase their spending to capture the right talent. This is, though, an area where a number of alternative solutions - Managed Security Services and using Generative AI to reduce toil, to name just two - exist, which may explain why nearly a fifth (18%) of organizations are decreasing their talent-focussed expenditure *(Figure 5)*. Indeed, Managed Security Services are one of the priority spending areas this year, with half of businesses already investing in these, and a further 40%planning to invest in them in the next two years.

Figure 4
Security spending

35% feel they overspent in the last 12 months

19% feel their spend was inadequate

76% will increase cybersecurity spending in the next 12 months up from **73%** in 2022

Figure 5
The fight for talent

↑ **48%**

Increased spend

↓ **18%**

Decreased spend

There are several ways businesses can look to reduce their security spending, Jay Coley - Sr. Manager, Technology Specialist Group - explains.*'When deciding their security budgets, businesses must undertake a thorough risk assessment to counteract spiralling spending. Without identifying priority risk areas, they may take the approach of combating threats as they arise, which can rapidly lead to escalating costs and a slew of tools which don't work together and are difficult to integrate into their existing stack.*

'One additional solution to rising budgets is to consolidate security toolings to work with a lower number of vendors. Not only will this help teams to control their security spending, it also significantly increases the likelihood the tools they use will integrate together well, creating a more coherent, more secure security stack to protect their business - all at a lower cost.'

Figure 6

Current and planned security investments

	Currently investing in	Planning to invest in within the next 12 months	Planning to invest in within the next 2 years
Firewall	61%	23%	10%
Network Security Monitoring tools	54%	28%	10%
Managed Security Services	50%	29%	11%
Remote employee security (onboarding and ongoing employee education)	50%	31%	11%
API security	46%	29%	13%
DDoS controls	44%	31%	11%
Digitisation of critical infrastructure	44%	33%	13%
5G security	41%	32%	13%
Defense against nation state attacks	38%	31%	14%
Generative AI	37%	36%	15%
WAF	36%	33%	13%
Bot mitigation	36%	32%	16%
Paved road/paved path solutions	32%	32%	15%

These current and planned security investments are highly diffuse, and cover a wide range of threats, indicating the extent to which security is a moving target for businesses. All of this points to a continued picture of uncertainty on how to take precise, concrete steps to mitigate cyber threats. The results of this are stark and clear, and businesses will continue to see their profits affected if they are unable to implement an effective cybersecurity strategy that acts as an enabler for innovation within businesses, rather than as a blocker.

In the face of this uncertainty, one potential solution is to partner with professionals who understand the objectives of an effective cybersecurity strategy is crucial. This will allow your business to both hit its security targets and avoid unnecessary costs, which are increasingly difficult objectives to marry as many security toolings become increasingly specific, more expensive, and more difficult to integrate into existing stacks.

However, the multitude of security providers in the market are often providing companies with conflicting advice on how and where to target their spending. To solve this challenge, businesses must be aware of their specific requirements and, where possible, trust their security teams to work with peers and consult expert groups to obtain the best information. This collaborative approach can go some way to mitigate the spiralling security tooling costs that can hit businesses as they try to solve their security threats.

Businesses will continue to see their profits affected if they are unable to implement an effective cybersecurity strategy that acts as an enabler for innovation within businesses, rather than as a blocker.

Has your cybersecurity footprint become too complex?

Many businesses will inform their cybersecurity strategy with a trends-based approach. This means they buy and implement new security tools on an as-needed basis - or, even worse, based on what they read in the media. The result of this is a security stack made up of disconnected, often poorly integrated tools that are unable to work to their maximum capacity.

Having your security stack set up in this way has several harmful effects. Primarily, by not fully deploying security tools - such as by running them in log-only mode - you miss out on any of their positive effects. Instead, in this state they exist only to point out threats after they have made themselves felt on your network. It is highly troubling that 45% of cybersecurity tools are still not fully deployed by the teams that use them, although this represents a significant improvement on 2022, when 61% of security tools were not fully deployed. Additionally, 41% of the tools cybersecurity professionals are using overlap in the protection they provide, resulting in continued overspend by security teams. The harmful effects of these habits are illustrated by the continued prevalence of false alerts, with a third (34%) of security alerts in the last twelve months a result of these. This is a slight decrease on 2022 (38%) but means that false alerts continue to occupy a major portion of security teams' available time. Again, all of this adds up to cost your organization significant sums of money and resources *(Figure 7)*.

Figure 7
Deployment of security tools

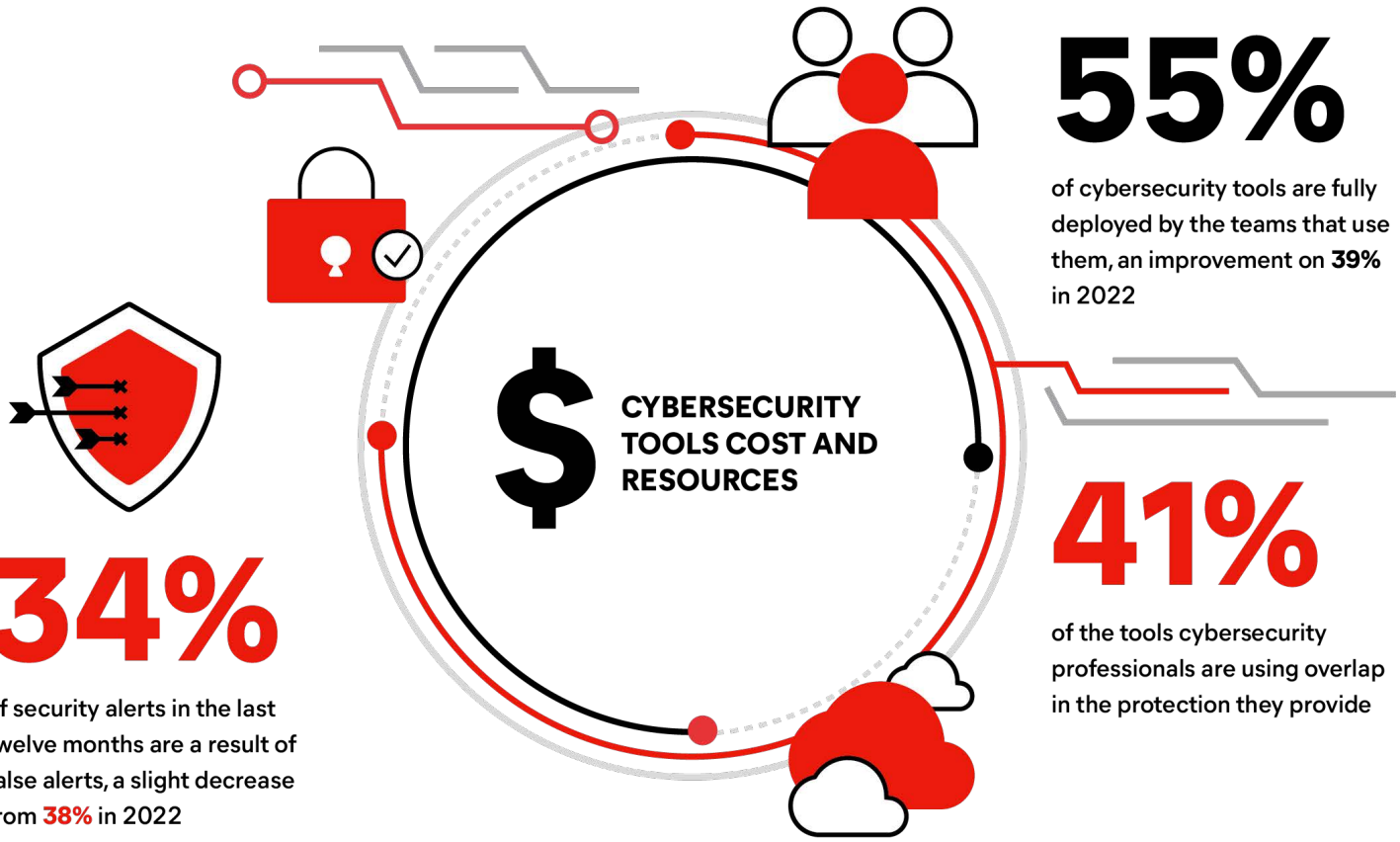
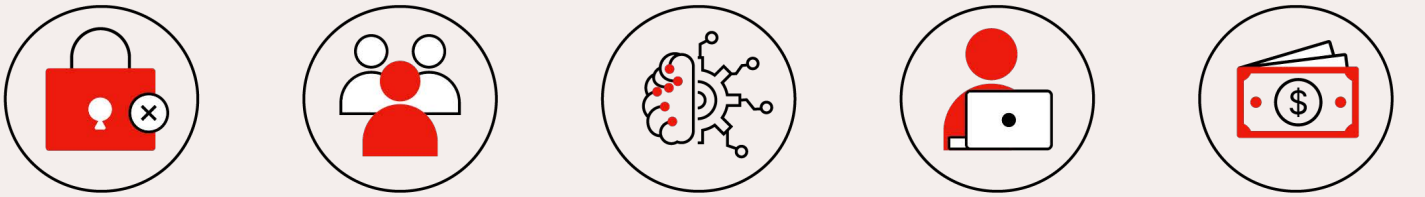


Figure 8
Areas of concern



36%
Sophistication of the threat landscape

36%
Lack of talent with relevant skills

35%
Generative AI

33%
Ability to secure remote workers

26%
Damaging results of inadequate investment

Outside of these material challenges, there is a wide range of concerns that are front and centre for cybersecurity professionals over the next twelve months. The principal area of concern is the sophistication of the threat landscape (36%), closely followed by the risks posed by Generative AI (35%). The ability to secure remote workers (33%) continues to provide a challenge, even as we move further from the pandemic, with a lack of talent with relevant skills (36%) also a major concern for security teams.

These concerns cover a wide range of worries - from internal practices through to emerging technologies - and each score incredibly closely to one another, indicating just how diverse the worries of security professionals are. An additional area of concern for many security professionals (26%) is the damaging results of inadequate - or misplaced - investment in cybersecurity technology. The mitigation of these negative results is a vital part of any security team's role and, so, ensuring that available budgets are not misspent on overly complex or poorly deployed solutions should be a major priority *(Figure 8)*.

So, how can businesses best use their cybersecurity budgets to ensure they are protected?

One potential response to this question is that organizations must avoid so-called 'integration by invoice,' where security providers wrap them up in any number of individual solutions that make them reliant on a single tech provider. Instead, businesses should target security solutions that are easily integrated into existing stacks, and which can be employed flexibly alongside existing systems. This approach can significantly reduce wasted spending on tools that never get used - or only get used ineffectively.

An alternative approach businesses can adopt is to look at Managed Security Services (MSS), which can significantly simplify their security footprint by working with trusted third parties. Nearly a third (30%) of the businesses we surveyed have begun to use these services in the last twelve months. The same amount of businesses have hired more cybersecurity specialists in the same time period. This demonstrates companies are beginning to recognize - and resolve - the existing gap in training and expertise and turning to Managed Service Providers (MSPs) and additional hires to address the expertise gap and reduce the risk caused by having an overly complicated cybersecurity posture.

But, to properly implement these changes, security teams must re-evaluate their security strategies to become less reactive. This will ensure they are able to avoid so-called 'integration by invoice,' where they are constantly tempted to buy new security products to respond to emerging threats. By shifting their security mindset to one that is more proactive, they can ensure their security tooling remains lean, simple and interoperable.

For example, vendors are expected to help their customers resolve a range of challenges, by providing ease of implementation, easy-to-use tools, integration and coverage across environments, and agility and flexibility in attack environments. The common outcome of businesses trying to leverage multiple 'best-of-breed solutions' is that each vendor's environment doesn't communicate with any others. This means that information about an attack detected in one cloud provider environment is often not immediately conveyed to other cloud environments within the stack. These lapses amount to a major tooling failure that businesses can avoid by simplifying their security footprint.

Generative AI: Useful... to an extent

The introduction of Generative AI is changing the ways industries across the tech ecosystem operate. And while much of the current conversation around Gen AI is exaggerated there can be no doubt that it is extremely effective at processing huge amounts of data in an instant. It is this capability that gives AI the power to make tangible improvements for businesses, particularly as they scale their operations.

When it comes to discussing its implications on businesses' security, however, Generative AI is largely being portrayed as a negative force. Our research among security professionals shows a more measured understanding. While they realize the potential challenges Generative AI can cause, placing it second on their list of threat drivers for the next twelve months, they are also well aware of the positive benefits Generative AI will bring to overworked, undermanned cybersecurity teams.

For this reason, Generative AI security is the top area security professionals will invest in over the next two years (50%). It is also the top security priority for businesses over the next 12 months (37%). Despite - or perhaps in anticipation of - this investment, 75% of cybersecurity professionals estimate Generative AI's impact will be positive over the next 12 months, rising to 77% over the next five years *(Figure 9)*. The one outlier in this prediction of positivity is Japan, where 45% of cybersecurity professionals anticipate Generative AI will have a positive impact in the next five years. This positive outlook provides a strong counterargument to the prevailing media narrative that Generative AI will open up numerous new threat vectors for bad actors to exploit, and put businesses at significant risk of cyber attacks on an unprecedented scale.

Figure 9
The impact of Generative AI

With this prediction of positivity, it is possible to reassess the narrative existing around the role Generative AI will play within future cybersecurity strategies. Above all, security teams will be able to leverage Generative AI as a useful tool for reducing toil. That is to say that Generative AI is no silver bullet for moonshot cybersecurity strategies - nor is it a poisoned chalice that bad actors will be able to exploit to bring down entire industries.

Instead, the benefits security professionals anticipate seeing from Generative AI are more banal, if no less useful for their teams. The greatest benefit these professionals expect to see is increased productivity (43%), followed by the ability to better protect their business (42%), and opportunities for increased innovation and new work (both 40%) *(Figure 10)*.

Figure 10
The benefits of Generative AI

These should all combine to create a more positive working environment for cybersecurity professionals, who have otherwise faced significant challenges in their day-to-day roles. Indeed, as well as reducing the time these professionals spend on busy work, the effective introduction of Generative AI will enable them to focus on the parts of their role that bring additional value to their organizations, significantly improving their experience of their everyday work.

This reduction of toil and mitigation of the challenges posed by the ongoing talent pool shortage is the key benefit Generative AI will bring to security teams. Of course, given the widespread proliferation of Generative AI within businesses, they must be aware of its potential risks. Indeed, businesses are already starting to implement concrete steps to ensure employees are educated about the dangers posed by Generative AI, and are ensuring the proper safeguards are in place to ensure rigorous security standards are maintained: 34% have company-wide AI policies, 34% have implemented specific training around Generative AI and 27% are using short-lived access tokens to authenticate users.

These preparations that businesses are already making for the introduction of Generative AI into their workflows demonstrate the measured approach the majority of organizations are taking towards the proliferation of Generative AI. They understand already that this will not alter the fundamentals of the cybersecurity ecosystem, and - in most cases - will be a net positive, removing much of the busy work that currently contributes to cybersecurity professionals being significantly overworked.

'AI tools will play a major role in reducing the workload for security teams,' Dr Liam Mayron, Staff Product Manager at Fastly, explains. *'There are several ways they can be used to do this, from generating reports - which are a crucial part of understanding security postures - through to trawling through huge amounts of data to gather contextual information to help businesses build data-driven cybersecurity strategies.*

'The use of AI and models built using Machine Learning also allows security teams to guide their processes to predict future threats, and inform their strategies based on these predictions. This targeted approach can be used to reduce the "spray and pray" security strategy many businesses adopt and, in doing so, reduce excess cybersecurity expenditure.

'Alongside these benefits brought by AI, Managed Security Providers can further help struggling teams both by taking on the burden of managing their security stack, reducing toil in the short term, and by helping with recruitment to ensure in-house teams are better placed to react to threats without significantly increasing the pressure on individual team members.'

Fixing the security talent shortage. Are you hiring the right experts for your roles?

The talent pool - and its limitations - is a critical theme highlighted by many cybersecurity professionals as an area for concern, requiring increased attention and budget. Exactly half (50%) of the professionals we surveyed in 2022 stated that training or acquiring cybersecurity talent was their priority over the last twelve months. An additional priority for these security teams was to improve their organization's overall security posture through a programme of training (44%), designed to make security more accessible at all levels of their business. This often overlooked aspect of the security puzzle is extremely important, particularly when employees at all levels are responsible for cybersecurity breaches.

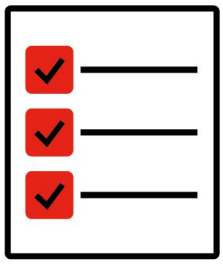
This training and recruitment drive has continued apace into 2023, with over a third (36%) of businesses continuing to place high-quality recruitment at the top of their investment wishlist for the coming year. Indeed, nearly half (47%) of the businesses we surveyed have increased their security talent spending over the last twelve months, indicating the willingness businesses have to spend significant sums to recruit the right people. However, this cuts both ways and also presents a challenge to businesses, which have to be prepared to spend huge sums to secure the right talent *(Figure 11)*.

This feeling can be particularly heightened when the talent entering the cybersecurity industry does not possess the relevant skills needed to succeed. 36% of cybersecurity professionals feel that new talent entering the industry does not possess the necessary skills, while nearly half (46%) feel they are unable to deal with threats derived from emerging technologies. In addition to these challenges, new talent is also perceived to lack experience working with technology at scale (36%) and in dealing with crises (35%), both of which are seen to make these new employees less than ideal when joining security teams *(Figure 12)*.

Figure 12
New talent skills

46% feel that new talent are unable to deal with threats derived from emerging technologies

36% feel that new talent entering the industry does not possess the necessary skills



36% perceive that new talent lack experience working with technology at scale

35% perceive that new talent lack experience in dealing with crises

Figure 11
Training and recruitment

of businesses continuing to place high-quality recruitment at the top of their investment wishlist for the coming year

of the businesses we surveyed have increased their security talent spending over the last twelve months

This situation is only exacerbated by the perception from some security professionals (27%) that a lack of relevant technical skills throughout their organizations will be a driver of security threats in the next twelve months. There is, therefore, a pressing need for improvements in recruitment, as well as organization-wide training. In much the same vein, 30% of security professionals feel that security issues in the last twelve months were directly caused by the talent shortage, with a third of them (33%) predicting this will continue to present a challenge in the next twelve months. This all adds up to demonstrate exactly how pressing the talent pool challenges currently facing the cybersecurity industry are, and how urgently they need to be resolved *(Figure 13)*.

It's vital to remember that many of these challenges are caused by the diversity of the cybersecurity landscape, and the specialized knowledge required to work to a high level within the industry. For example, an endpoint expert is not going to understand application security. It's too simple to propose a catch-all solution for the myriad challenges within the industry. But there are some steps businesses can take to address the difficulties they face with the talent pool shortage.

One of these is to prioritize cross-organizational security. This is a combination of both hiring the right experts - who understand emerging technologies - and implementing rigorous internal practices to ensure your business is protected from the widest range of threats possible. Over a third (37%) of cybersecurity professionals highlight closely defining this new security approach - especially as it relates to emerging security challenges, such as Generative AI - as a priority, indicating the widespread nature of cross-organizational security. The other side of this coin is the prioritization of improvements to their organization's cybersecurity skills through training and talent acquisition, which the same number (37%) of security professionals identify as a goal for the next twelve months.

An alternative option businesses can take is to leverage the benefits provided by Generative AI to reduce the strain their security teams face. 43% of security professionals expect the proliferation of AI technology to increase productivity. This is thanks to the significant load AI tools can take away from security professionals by taking procedural, time-consuming tasks away from them. After all, there is a clear desire from cybersecurity professionals for AI tools to take on the brunt of the basic work, allowing them to focus on more valuable work.

Figure 13
Issues of talent shortage

One area where the benefits of Generative AI are likely to be seen is in the implementation of organization-wide training programmes. 35% of security professionals predict that Generative AI will allow them to more effectively train their colleagues in the fundamentals of cybersecurity, which will offer them significant support fostering security-first mindsets throughout organizations. An additional benefit of this is the time Generative AI can save for these overworked professionals who would otherwise invest significant time into developing training programmes. The content development potential offered by Generative AI will go a long way to reducing this time requirement and, as a result, allow security professionals to focus on keeping their organizations secure.

35% of security professionals predict that Generative AI will allow them to more effectively train their colleagues in the fundamentals of cybersecurity.

It is clear that businesses are taking active steps to resolve the challenges facing them that are related to the talent pool. But in an increasingly diverse cybersecurity landscape, many in-house security teams are struggling to keep pace with changes. Additionally, new, inexperienced hires are finding it difficult to find their feet in the industry, due to several factors. So, how can businesses resolve these challenges?

The overall goal of these security strategies is to improve security postures throughout an organization. One key aspect of this is accessibility. Regular workers must be able to understand why they have to do what they have to do to keep their business secure. For this reason, it's encouraging to see that 35% of security professionals are aiming to make cybersecurity more accessible in order to meet usability requirements to boost their cybersecurity posture. This is a strong move to counteract the perceived danger posed by employees who do not understand their security obligations, and a clear sign of the scope needed to build and implement an effective cybersecurity strategy, and solve the challenges posed by the ongoing shortage in the talent pool.

The growing prevalence of Managed Security Services and why they might be the answer to your security woes

An alternative solution to the various security challenges facing businesses is for them to take those challenges off their hand, and work with a trusted partner to manage their cybersecurity. After all, in-housing security is hard, so businesses - particularly those unable to dedicate adequate budget to security strategies or those looking to alleviate some of the load on their security teams - should consider the benefits provided by third-party security solutions.

This increased trend towards Managed Security Services (MSS) is demonstrated by the top investment areas for security teams in 2023, with 30% of businesses beginning to invest in MSS over the past twelve months. Additionally, MSS is a new entry among the top areas for planned investment in 4th position - behind firewalls (1st in 2022), network security monitoring tools (2nd), and remote employee security (3rd). This shows that - outside the basic tools needed for cybersecurity - MSS is the most popular area for planned investment, as businesses increasingly look to industry experts to take on their security burden.

Figure 14

Businesses plan to focus their spending on the following areas over the next 24 months

2022			2023			
1	46%	5G Security	1	51%	Generative AI security	NEW ENTRY
2	46%	Bot mitigation	2	48%	Bot mitigation	DOWN ONE
3	43%	Digitisation of critical infrastructure	3	46%	Digitisation of critical infrastructure	DOWN ONE
4	41%	DDoS controls	4	46%	WAF	UP TWO
5	41%	Defense against nation state attacks	5	45%	5G Security	DOWN FOUR
6	41%	WAF	6	45%	Defense against nation state attacks	DOWN ONE
7	41%	Endpoint detection and response tools	7	42%	Remote employee security	UP FIVE
8	40%	Web Vulnerability Scanning Tools	8	42%	API Security	UP FIVE
9	40%	Network defense wireless tools	9	42%	DDoS controls	DOWN SIX
10	40%	Managed Security Services	10	40%	Managed Security Services	NO CHANGE

Indeed, in another positive sign for those security businesses able to provide their customers with MSS, 47% of security professionals say that their organization's cybersecurity strategy has hampered business innovation. Given security is supposed to be a business enabler, this number is alarmingly high, and there are a number of potential causes for this feeling.

These roadblocks to innovation can make their impact felt throughout a security stack's lifespan, but are particularly common at the implementation phase.

The first of these is poor communication. Whether this refers to inadequately communicating the ways new security tools will affect existing workflows or ineffectively educating stakeholders on the objectives of a security strategy, a poorly communicated cybersecurity strategy will never encourage innovation. Instead, team members need to be consulted at all stages of the implementation of any tool - or, indeed, any new way of working, such as when a Shift Left mentality is adopted by an organization. In these instances, communication - and a joined up approach - is key to ensuring operations continue to run smoothly throughout a business, even as ways of working change.

An additional blocker to security acting as a business enabler is insufficient budget or tools. This often leads to incomplete or botched integrations - and leaves businesses with holes in their security tooling.

There is one overarching theme that links these other roadblocks. When stakeholders are misaligned on delivery of a business' security strategy, it is rarely going to allow the employees of that company to innovate. This can be the result of a lack of communication over objectives, implementations, or scale and scope but can also be caused by budget availability, and several other factors. At the end of the day, any new project requires full buy-in from its stakeholders and, when this applies to the security stack, that often means securing full, organization-wide cooperation to see significant success. The mitigation of these miscommunications and differing goals is one benefit of MSS, and a clear reason why businesses should increasingly look to include third-party solutions in their security stacks.

Regardless of your industry, it's important to understand the threats you face

In every industry vertical, understanding the unique environment impacting their cyber security outcomes and plans is essential. In this section, we delve into the key findings tailored to four distinct industries: Finance, Retail, High-Tech, and Media. Read on to gain valuable insights into the unique challenges and strategies associated with each sector:

Finance

The financial sector continues to be targeted by financially motivated organized crime, which often takes the form of data breaches, identity-based threats - such as malware, phishing, and social engineering attacks - and hacking, through the use of stolen credentials. Additionally, financial organizations each suffered an average of 50 known attacks in the last year - more than any other industry. For this reason, financial and fintech professionals we surveyed are overwhelmingly (80%) choosing to increase their security spend to try and secure themselves.

This increased spending comes despite the fact that only 53% of finance professionals surveyed believe their organization has fully active cybersecurity tools. The results of this have carried significant implications for the number and scale of cyber attacks these businesses have suffered. In the last twelve months, 29% of these businesses have suffered from a DDoS attack, 27% have been affected by open source software vulnerabilities, and 24% from an API attack, all resulting in network outages or downtime, data loss, and financial damage.

There is, however, significant reason for these professionals to be optimistic about what the future holds for their cybersecurity posture. Financial professionals are more likely than average (85%) to appreciate the positive benefits Generative AI will bring to their workplace, and recognize the growing influence this will have in unlocking new job opportunities in their sector. As part of this drive, businesses in the financial sector are more likely than their counterparts in other industries to increase their talent spend, with 56% prioritizing this. An extension to this recruitment drive is the expansion of organization-wide security protocols, with a drive from 40% of businesses to make their security more accessible to increase its usability. This is a vital consideration as Secure by Design - the elimination or reduction of hazards by design - increasingly becomes the norm, meaning all employees will need to understand the basics of cybersecurity.

Retail and eCommerce

Suffering on average 41 known cyber attacks this year, businesses in the retail and ecommerce space have taken a different approach to many other sectors by focussing their hiring efforts on recruiting cybersecurity specialists (37%) to a greater degree than other industry verticals. This increased specialism is reflected in the fact that only 3% of ecommerce businesses are reducing their talent spend - compared to an average of 18% across all other industries - and also in the fact that ecommerce is the industry where security teams are most likely (43%) to attribute security breaches to a lack of internal education. Simply put, many of these businesses are still laying much of the groundwork for a successful cybersecurity strategy.

This all points to a recognition of the vital data these businesses handle on behalf of their customers. The key danger posed to retailers in the last twelve months has been data loss resulting directly from a cybersecurity breach - 46%, compared to this affecting 29% of businesses across all other industries. When customer information is at risk, so is customer trust. The fallout from security breaches can therefore be significant, affecting not only existing customers but also costing retailers potential future business. As the retail industry continues to be impacted by a variety of threat actors that leverage a range of tactics such as deploying malware to capture credit cards being processed by webforms and more common tactics like phishing, these impacts are only being more keenly felt.

High-Tech

With businesses in the high-tech industry suffering an average of 48 known cyber attacks this year, organizations in this sector have slightly different worries to those in many other verticals. Above all, they are more concerned about ransomware (32%) and DDoS attacks (27%) than other industries (26% and 20%, respectively), indicating their awareness of the dangers caused by social engineering attacks targeting individuals, as well as those of at-scale attacks, and their need to be able to protect themselves against both.

This recognition of the range of cyber threats that businesses face in the modern threat landscape offers a likely explanation for high-tech businesses' less optimistic outlook on the role of Generative AI than other industries. 69% of these businesses see Generative AI as a positive for security, compared to 75% across all other industries. This is likely a result of the role Generative AI can play in both scaling attacks, and writing increasingly sophisticated content for social engineering attacks.

In the next twelve months, the high-tech industry's primary focus will be on defining a robust approach to overcoming new and emerging cybersecurity threats, such as Generative AI. Alongside this priority, high-tech businesses also expressed the importance of improving cybersecurity skills through training and talent acquisition to protect their entire team, regardless of whether they are remote, hybrid or in-office.

Media

Of all the industries featured in this study, businesses in the media suffered the fewest known attacks, experiencing an average of 25 of these in the last year. While this would seem to indicate that these businesses are more secure than those in other industries, the outcomes from these attacks have been significant.

Media organizations hit by cyber attacks are the most likely to suffer serious financial damage as a direct result (36%, compared to an average 23%). The immediacy of this outcome likely offers some explanation as to why media organizations are more likely than any other to invest in Managed Security Services (56%). They need urgent solutions, and cannot afford to wait for their own security teams to take control. This may also represent an attempt to patch over a lack of spending in the past year, with 28% of media organizations feeling their spend was inadequate, compared to an average of 19% across all other industries.

Above all, it seems that despite the low number of cyber attacks these businesses face, there still remains significant work to be done to remedy lingering security challenges, and mitigate the effects of previous, less effective strategies.

Secure by Design: The cost-effective mentality placing security at the heart of organizations' stacks

The most common solution businesses propose to the range of security threats that exist today is to throw money at them. The results of our research demonstrate this with the vast number of businesses who continue to escalate their security budgets each year, especially around Generative AI and in their recruitment cycle. There is, though, an alternative pathway many of these organizations can take to both ensure their security, and combat spiralling cybersecurity costs.

This approach - Secure by Design - is part of the Shift Left mentality, whereby security is a core consideration from any project's outset. This ensures any developments or updates are always made with security in mind. This approach frees developers to innovate within a safe environment, going a long way to resolve the perception of security as a blocker to creativity that often exists within businesses.

Secure by Design represents a rethinking of cybersecurity to remove responsibility - and therefore blame - from individuals by designing systems that have resilience baked into them. This all serves to create a secure environment where the excess costs caused by reactionary security strategies and constant tool integrations are avoided.

Kelly Shortridge, Senior Principal Engineer (Office of the CTO) at Fastly , explores the 'Secure by Design' mentality, and how it marries security with speed, enabling developers to innovate effectively while also keeping their organization safe.

Secure by Design has been the dream since the golden era of computer science in the 1970s and 1980s[1]. It's now a call to action from government agencies representing 32 countries[2]. But what does it mean in practice? How must organizations transform to pursue it?

Secure by Design means we eliminate or reduce hazards by design. It means our security success does not depend on human perfection to succeed – that we don't need in-the-moment human action to uphold security. Secure by Design means we weave resilience into the fabric of our systems rather than trying to add it after-the-fact through warning systems or administrative controls (like policies or "awareness" training).

Secure by Design means we work with human behavior, not against it. The reality is, as humans, we're always stressed or distracted or under-caffeinated – our decision-making will never be perfect. Our employees and users are not security experts, nor should they have to be. Their goals are never security in and of itself. Secure by Design means we are the ones who ensure that we build, deploy, and deliver our systems with security properties that make the system more resilient to attacks.

Whenever we hear something failed due to "human error" or a problem persists because "humans keep doing X wrong," we should re-characterize the problem as a poorly-designed system, tool, or environment[3]. It's a call to action to refine design so the secure way is the easier, faster way.

Why do we want this? We want reliable, trustworthy services – we want to ensure our software works as intended, to ideally exceed our users' expectations. Secure

by Design sustains this reliability and trustworthiness, to succeed in our organizational missions despite the presence of attackers.

Secure by Design gives us confidence that, even when attacks happen, the impact will be minimal. It also enables innovation by removing the need for humans to worry about security in the course of their work; they are instead free to focus on their unique value creation for the organization.

As organizations increasingly become digital and write software in-house, Secure by Design is even more important for security leaders to prioritize. Traditional security solutions often hurt developer velocity – but your organization needs to be delivering code to differentiate now more than ever. Secure by Design aligns security with speed.

How does Secure by Design look in practice? We can either eliminate hazards by design or reduce the hazardous methods and materials we use.

Solutions that **eliminate** hazards by design feature two key traits:

- They do not depend on human behavior
- They provide complete separation of the user from the hazard

Think of customer payment data. Rather than prescribing secure development training or vulnerability scanning, we could work with the engineering team to break apart the application into a more modular architecture to isolate access to payment data. That way, only the billing service can access that data; all the other services will not have access to it. Or, we could outsource payment data handling to a third-party provider – eliminating the hazard by not even storing or handling payment data in our systems.

Solutions that **reduce** hazards by design allow us to substitute less hazardous methods and materials. Hazardous methods in software take the form of "don't roll your own X" – whether X is cryptography, database, logging pipeline, observability, and other middleware that requires specialized expertise to build it safely. They can manifest as injection from an attack perspective; for instance, we can consider SQL injection as the result of "rolling your own" database query builder.

To reduce these hazardous methods, we have a few opportunities at our disposal. For most organizations, their market differentiation does not come from solving distributed systems or security problems. We can standardize and "choose boring" technology where we can, outsourcing hard software and systems problems to vendors possessing the necessary expertise (like outsourcing caching to a CDN like Fastly).

Hazardous materials include code in languages lacking memory safety, like C or C++. To reduce these hazardous materials, we can refactor our systems into a memory safe language or isolate unsafe code, such as wrapping it in a WebAssembly sandbox (which is what happens by default when you run your C code, and other code, on Fastly's Compute platform).

More generally, hazardous materials reflect any technology – whether libraries, frameworks, code snippets, and more – that is difficult for us to understand. If we can standardize on technologies that are well-understood and easier to maintain, then we can reduce those hazardous materials. For example, we can build a standardized authentication component (known as a "paved road") that developers can place in front of their app (such as by running it on Compute as an edge service); that way, the developer doesn't worry about writing their own auth logic – which also means fewer mistakes or misconfigurations.

---

1 Example: Saltzer, Jerome H., and Michael D. Schroeder. "The protection of information in computer systems." Proceedings of the IEEE 63, no. 9 (1975): 1278-1308. https://www.cs.virginia.edu/~evans/cs551/saltzer/

2 USA, Australia, Germany, Canada, UK, Singapore, New Zealand, Norway, Israel, South Korea, Japan, Netherlands, Czech Republic, and CSIRTAmericas (includes most of North, Central, and South America – represents 19 countries in addition to USA and Canada)

3 https://www.visualexpert.com/why.html

4 https://mcfunley.com/choose-boring-technology

Methodology

The survey was conducted among 1,484 IT decision-makers (more than 2/3 respondents directly make or influence cybersecurity decisions) in organizations with 500+ employees (250+ for Australia/New Zealand) across Japan, US, DACH, UK & Ireland, Spain, Australia/New Zealand, and the Nordics. Participants hold a wide range of roles across the infrastructure including cloud operations, IT management, application architect and security operations analyst.

The interviews were conducted online by Sapio Research in August, September & October 2023 using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 2.6 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Sapio

Best new agency finalist, Sapio is adept at opinion polling (we have access to 80 million people internationally), focus groups, face-to-face interviews, telephone interviews, online research, desk research and statistical modelling to mention just a few techniques. We love B2B research and consultancy. Our business is based on partnership principles inspired by social enterprise.

About Fastly

Fastly is a global edge cloud provider that offers different solutions in the areas of edge computing, network services, which includes content delivery (CDN), observability, and security. Fastly's powerful and programmable edge cloud platform serves the most demanding Internet industries: media, e-commerce, broadcasters, travel booking wholesalers, fintech and large high-tech companies, among others. Fastly helps the world's top brands deliver the fastest online experiences possible, while improving site performance, enhancing security, and empowering innovation at global scale. With world-class support that achieves 95%+ average annual customer satisfaction ratings, Fastly's suite of edge compute, delivery, and security offerings has been recognized as a leader by industry analysts such as IDC, Forrester and Gartner. For more information on our mission and products, visit **www.fastly.com**.