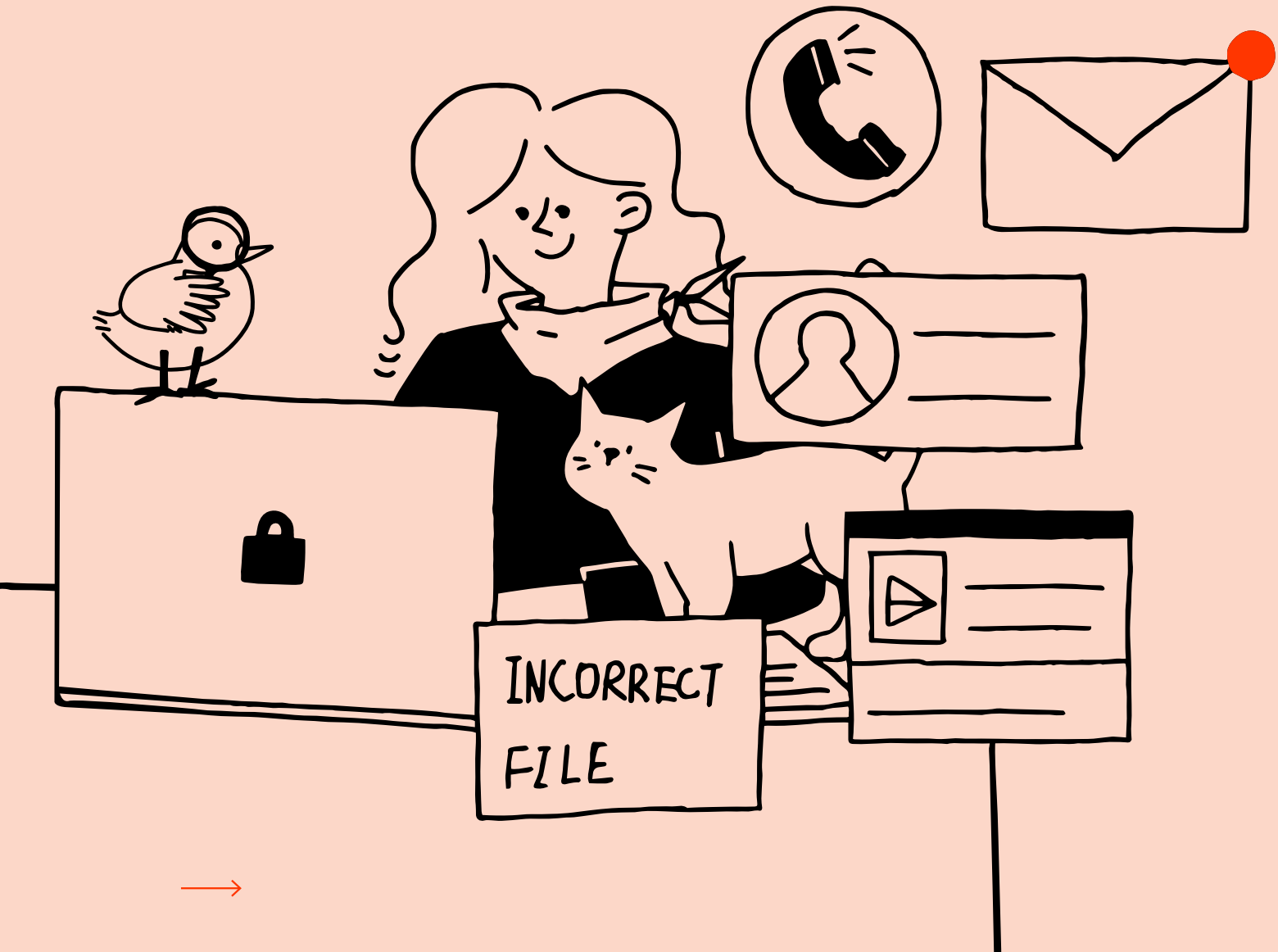
zivver

Cybersecurity Trends 2024



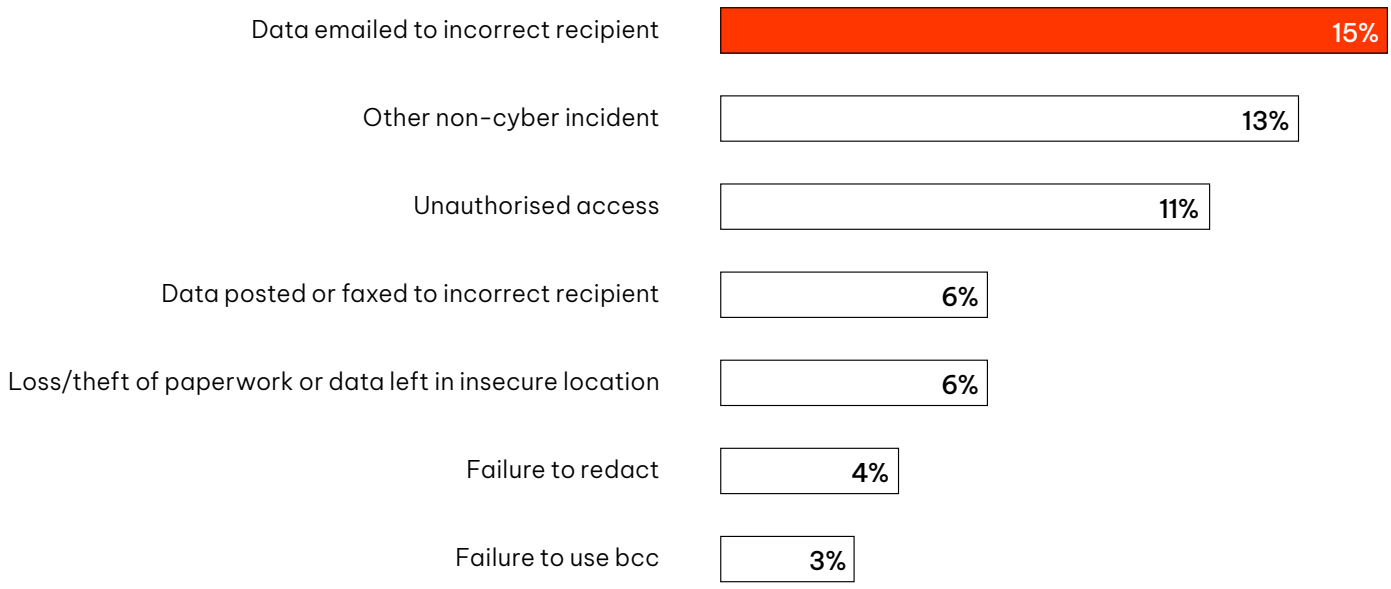
Executive summary

Oliver Brown | Vice President of Commercial

According to the latest data, over 45,000 data incidents have been reported to the ICO since 2019. Of these, a huge 75% are the result of non-cyber related causes – incidents for which there is no clear link to a malicious cause.

This is not new or surprising information. We know that email and communication platforms remain the largest risk vectors, and employees continue to make mistakes when managing sensitive data.

In 2024, security will be considered a tactic for success, rather than an afterthought. To combat risks and fortify areas of weakness, security must be embedded into every individual and team strategy. But that isn't to say that security should come between people and productivity.



over **45,000** data incidents have been reported to the ICO since 2019

The world of security has moved on from compulsory awareness training. Traditional security policies gather dust while people navigate restrictive guidance on the do's and don'ts of sharing sensitive information with their stakeholders. IT teams are losing confidence in people to behave securely; people are losing patience with non-user friendly tech.

2024 will see cybersecurity become a collaborative effort for many progressive organizations. In order to keep up with the evolving security landscape and protect the security of their digital infrastructure, (think the development of AI and LLM, issues of interoperable tech, restrictive budgets etc), security and compliance leaders must bring every employee along on the security journey.

It's time for change.

Read on to investigate how the cybersecurity landscape is evolving for the better, with insights from security leaders on:

- Who is ultimately responsible for an organisation's security
- How to build a collaborative culture around compliance
- Building risk-centric strategies tailored to employee needs
- The role of technology in meeting evolving compliance laws
- How to measure the success of security training
- AI, LLM, and the importance security-by-design

Chapter 1:

Giving control back to IT leaders

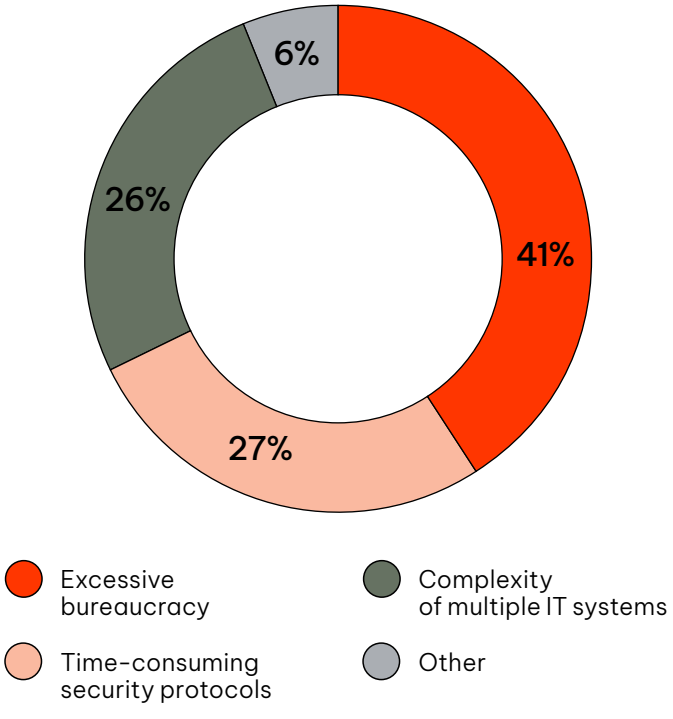
Adam Low
Chief Technology Officer

In an era in which IT and data security risks are escalating in breadth and scale, the role of IT security leaders has never been more critical. The landscape of IT security is rapidly evolving, compounded by the proliferation of IT systems, applications, and tools. One challenge I regularly hear from security and IT leaders is their inability to be in one hundred places at once. They cannot oversee the use of all applications, overlook every employee's shoulder, or keep an eye on all the potential inbound or outbound security risks to pose a threat to their organization, whether malicious or on the inside. This expansion has created a hotspot for malicious actors who increasingly target employees as gateways into organizational systems.

And so the pressure on IT security leaders is immense. With the threat landscape expanding at an unprecedented rate, the task of safeguarding data and systems has become increasingly daunting. This challenge, though formidable, is a testament to the critical role these leaders play in our digital world, and the need for control over their cybersecurity strategies.

More platforms, more problems

However, our current approach to IT security is not without its pitfalls. Research indicates that employees often feel burdened by security processes, fostering a culture of fear, blame, and disrupted workflows. According to our findings, the most significant barriers to work employees face include excessive bureaucracy (41%), time-consuming security protocols (27%), and the complexity of multiple IT systems (26%).



And, when employees feel hindered by tech, often they seek out alternative (less secure) ways of working, turning to non-compliant and unsecure communications platforms. In fact, a startling revelation from a recent Gartner report shows that 64% of employees routinely bypass security measures, with 9% acknowledging the heightened risk this poses to their organizations. This behavior underscores a disconnect between security policies and practical workflow integration.

During a recent industry debate, we questioned the notion of universal accountability for security. The consensus? While everyone bears some responsibility, simply delegating this accountability without proper support and tools is a recipe for failure.

People will inform the procedures

In 2024, security leaders must lead their organizations in the adoption of a more collaborative approach. By involving employees in the creation and review of security policies, we can improve both the practicality and adherence to these controls. Engaging employees to understand specific risks in their areas of work fosters a culture of mutual respect and shared responsibility.

Key to this is secure, user-friendly tools that cater to both usability and security needs. This approach not only enhances security but also reduces the likelihood of employees resorting to unsecured alternatives.

It's essential to maintain a balance between empowering employees and retaining the core responsibility of the security team. Establishing channels for ongoing feedback on security policies and tools allows for adaptability in the face of evolving security challenges.

In conclusion, transforming our approach from imposing rules to fostering a collaborative environment can significantly enhance our IT security posture in 2024. By treating employees as allies and equipping them with the necessary tools and knowledge, we can create a more robust, security-conscious culture. In this evolving digital landscape, collaboration is not just beneficial—it's essential for the future of IT security.

Key takeaways:

Security is not a one-man game – nor is it a one team game

Collaboration is key: security leaders must foster an organization-wide security culture with buy-in from exec-level down

Finger-pointing gets you nowhere.

Employees are not threats to be mitigated; they are your greatest line of defense and must be empowered as such

Acknowledge the vital role of tech in your security posture.

A focus on cohesion between people, processes and technology will support IT teams in identifying and preventing threats

Chapter 2:

Striking the balance between risk-centric strategies and employee-centric solutions

Anita Mavridis
Vice President of Product

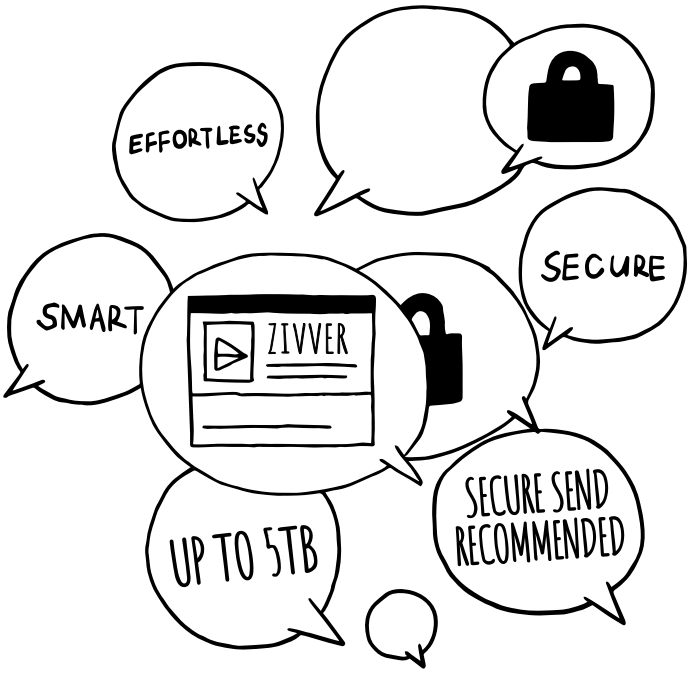
To truly empower efficiency and security, organizations must adopt a risk-centric approach.

Information is the lifeblood of businesses, serving as both our most valuable asset and our most significant liability.

Human error remains the leading cause of data incidents – this is no secret. This harsh reality not only compromises sensitive information but also leads to a growing rift between IT leaders, employees, and data protection practices. The result? Inflated technology stacks, excessive spending, and dissatisfied employees.

The real question is, how can organizations manage their technology investments to maximize value, minimize risks, and bridge the gap between employees and IT leaders? The answer lies in truly understanding the 'why', aligning your technology with the 'how', and understanding your ROI.

Let's dig a little deeper.



The why:
Risk-centric strategy

To truly empower efficiency and security, organizations must adopt a risk-centric approach. By identifying the primary risk vectors, organizations can focus their security strategy and allocate resources where they are most needed. Start with the 'why' – understand why your data protection measures exist and what you need to protect.

The how:
Employee-centric solutions

According to Gartner, by 2027 50% of large enterprise CISOs will adopt human-centric security design practices. Empowering efficiency involves acknowledging your employees' needs, understanding the data they handle, and their business processes. In practice, this means selecting security solutions that enhance the user experience, not hinder it.

A security solution is only as strong as its user adoption. In a world where remote work is prevalent, a frictionless, user-friendly experience is critical to prevent shadow IT, ensure compliance, and protect your reputation.

Calculating ROI
of security measures

Adopting technology is a significant financial investment, and now more than ever, IT leaders must justify these expenditures. Unlike some investments where the returns are easily quantifiable, the benefits of security solutions often involve intangible aspects such as reduced risk, enhanced reputation, and increased customer trust. These can be challenging to translate into concrete financial metrics.

Do yourself a favour and invest in security solutions that offer actionable insights enabling you to monitor the impact of your investment, and continuously assess whether they are delivering the expected value. Regular audits and feedback loops are essential for ensuring your tech stack aligns with the 'why'.

In conclusion, the road to empowering efficiency and ROI in data protection starts with understanding the 'why' and proceeds with aligning your technology with the 'how.' By focusing on risk vectors, prioritizing employee needs, and measuring ROI, organizations can create a harmonious environment where technology and security solutions truly empower people.

Key takeaways:

Quantifying the value of your cybersecurity investments incorporates intangible aspects of your business, including reputation, employee satisfaction and stakeholders. Implementing solutions which provide actionable insights on risks avoided helps IT leaders to communicate the value of investments to the wider business

Adopting a risk-centric approach ensures investments are centered around the needs of the user

User-adoption is integral; understanding employee needs will ensure technologies meet those needs

Chapter 3:

Security is a team sport in 2024

Nadine Hoogerwerf
Chief Information Security Officer

2024 promises to be an interesting year for cybersecurity and compliance. Developments that have been ongoing for a while will continue to drive cybersecurity risk and work in the coming year and beyond. The amount of risks to manage and work to do requires an 'all hands on deck' approach toward security.

Security regulations promote better security

The EU is clearly on a mission to upgrade cybersecurity from a nice to have to a must have for more organizations and governments. The NIS2 is applicable to a broad range of sectors and sets out minimum standards for security for organizations and EU member states. It is promoting both preventive and responsive measures and pays specific attention to security around communication and ICT products. An extra incentive for organizations to act on this is the personal liability: "Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive" (Article 32.6).

In addition to the NIS 2, the EU has worked on more specific legislation such as DORA, targeting IT risk management in the financial sector, and the Digital Service Act that aims to protect the rights of users of online services.

Of course, data protection professionals and their organizations must support these developments; it is critically important that sensitive information and processes are sufficiently protected against harm, abuse and unfortunate mistakes.

However, this development poses a challenge for many in the cyber security field who are already struggling on a daily basis to identify what to prioritize.

Yes, compliance with legislation and regulation are important because non-compliance may harm your business and/or lead to formal warnings and fines. Furthermore, focussing on compliance can be an effective way to improve security.

> The time security was done by a few individuals tucked away in an office somewhere is over.

Emerging technologies demand security attention

Still, compliance does not equal security. Cybersecurity teams should give attention to other developments, too. New technologies have been introduced (and are expected on the horizon) that will impact security significantly.

Take, for instance, AI technologies; these can be used by hackers to improve their phishing emails or scripts, making the 'job of a hacker' less dependent on skills. In addition, quantum computers are expected to be able to break several encryption algorithms that are frequently used nowadays, and are expected on the market within 10 years.

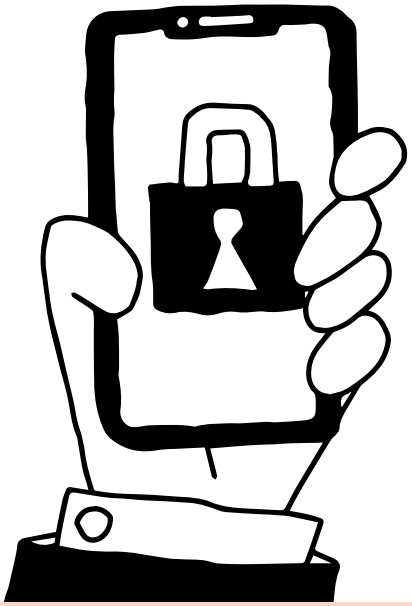
But, if we are being honest, it is not just new technologies that need security. Many existing technologies could still use a security upgrade in most organizations: the 'internet of things', web applications, email – the most common platforms and the most common risk vectors.

All hands on deck

In order to cover it all, security professionals should empower the whole organization to get security right. The time security was done by a few individuals tucked away in an office somewhere is over. Security should be part of everyone's job and on everyone's mind.

The security team should focus on enabling their colleagues to easily add security to their jobs. For example by providing code scanning tooling that can be executed by developers themselves before releasing their new code and software that can detect potential data leaks before they happen.

In addition it is key to install a tiny bit of security paranoia and a lot of security wisdom in your whole team. By awareness activities and by close collaboration with the security team everyone should be enabled and inspired to become a 'risk spotter' and a wise decision maker when it comes to security risk. Don't see the team as a liability, but as the security team's eyes and ears.



Key takeaways:

Compliance doesn't equal security

Some of our most frequently used platforms require security advancements to make them compliant – this should be a priority for every organisation for 2024

Compliance cannot be the responsibility of one team or individual; it is a company-wide priority for which everyone is responsible to some degree

A CISO's perspective:

Balancing the ad-hoc and the strategic

Anyone working in cybersecurity will know this feeling. It is 6pm and another day has passed. You are not sure how this happened and part of you feels like you just started the day. You look at your to-do list and see some important items still standing there. And to be honest they have been there for a while. Sure you have done a lot of work today, you have answered questions regarding the safe use of new tooling, have reviewed a proposal from another team and identified the security risks, you have explained (again) why you have not (yet) approved a new workflow. But the things that you did not do today were the things that you know in the back of your head are critical for the midterm security. And yes they have been on your list for a while.

As a CISO it is important to have control over your work. To make time to assess risks, to assess the changes in the field and/or within your organization and to study new regulations like NIS2 and DORA and new technologies like AI; to create an understanding of the implications for your organization, for the data and processes that you need to protect. And from that understanding, define what you need to do to keep the security levels at the same level or (if you are feeling bold) improve levels further.

This is a time intensive activity that requires focus and some peace of mind – two things that are very hard to come by as a CISO.

It is a critical part of the job. Yes, as CISO you can be the chief firefighter but you are also in the lead for preventing fires and, nowadays, are expected to be a business enabler, too. While you will receive support and maybe even applause when you put down a fire or identify a new business opportunity, you are usually not winning the popularity prize when you are working on preventing problems. Still if you as a CISO truly feel the ownership over the protection of your organization, you will prioritize this.

1

Reactive:

Your colleagues came up with a great plan and you share recommendations on how to mitigate the associated security risks.

2

Proactive:

you assess the organization's risks and threats and you build defense in depth.

It is important to make time for the proactive approach. The benefit of focussing on defense in depth is that it will offer protection against a wide range of threats including unknown threats. Defense in depth is about adding layers of defense. If one of your protection layers fails, nothing is lost and/or the blast radius is limited due to the other layers. In this way preparing for mistakes, oversights and insufficiencies.

As a CISO you may not know everything that is going on within and around your organization, you may not fully understand new technologies, you may not know all the details of the new regulations coming your way yet, but at least know your critical business processes, your most sensitive data and the core risks in this regard.

Stay focussed on those core risks and processes and add layers of defense so you can be prepared for the expected and unexpected fires.

Chapter 4:

Harmonizing training and tech to build a security minded culture

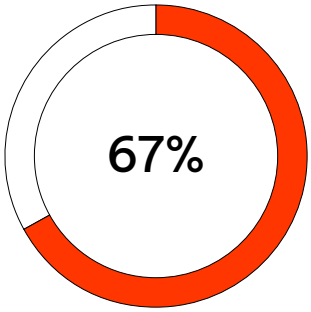
Rick Goud
Chief Innovation Officer

Organisations continue to invest thousands every year into training activities; compulsory courses, videos, quizzes... But how do you know whether your security training is delivering value?

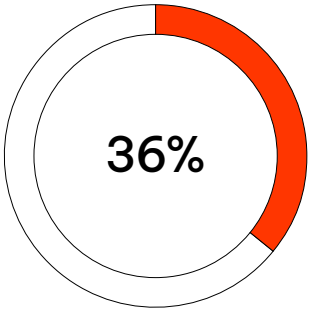
The delivery sometimes changes but the results rarely do. Employees may temporarily change their ways, but their behavior in the long term remains the same.

But that isn't to say that people intentionally ignore or forget their learnings. The issue is that training, in both its content and delivery, rarely meets the needs of people.

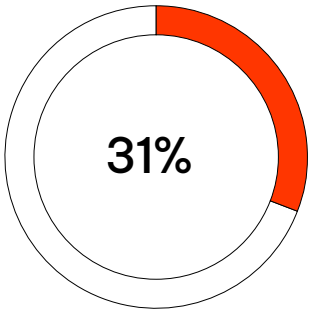
> Human error remains the leading cause of data incidents.



of employees have received some kind of data security training in the last two years



say they have used their learnings in their core role



haven't used anything they have learnt in their core role*

A new measurement for training success

For many organisations, training continues to be treated as a tick-in-the-box exercise for meeting their responsibilities under data protection regulations. Often, little thought is put into the real purpose of training or the measurability of its success.

In most cases, the actual delivery of training is considered the success metric: did all employees complete the training? Yes. Success.

However, if security incidents continue to happen, training must be challenged, not people. And this is the take away for 2024. Success must be measured on the success of people – not the delivery of training itself.

Human error remains the leading cause of data incidents. These incidents happen quickly, with an accidental click in the midst of a busy moment. Employees want actionable insights that will empower them to work efficiently and securely. This includes lessons on how to avoid landing themselves – and their organisations – in hot water. Making employees aware of the most prominent security risks they will face every day (such as how to use bcc properly, when to encrypt data, or how to share sensitive information compliantly) is a step in the right direction in ensuring training truly meets the needs of people.

Delivery of training

A one size fits all approach to training doesn't work. Across your organisation, employees have different responsibilities, priorities and stakeholders. They use different systems and have access to different data sets. Naturally, for every team and individual, the risk factors are different.

Training must be tailored to the individual. But exactly how practical is this?

Rather than taking a siloed approach, progressive organizations are collating their resources and technology to deliver in-the-moment training for every employee. Harnessing behavioral insights and intuitive technology, organizations can empower their people to work securely supported by in-the-moment threat and error prevention, and security best practice.

This approach, combining technology and knowledge sharing, delivers measurable security training for every employee, without impacting existing workflows or interfering with busy schedules.

In addition to the end-user benefit, targeted training supports security leaders to learn from their people. Identifying risk enables you to prevent data breaches, enhancing security in the vulnerable areas.

Your security training should do more than support people to identify phishing emails. It should drive your organization to adopt a sustainable data-driven security posture, in which every employee is empowered to work securely and with confidence.

Key takeaways:

The success of a security training programme should directly correspond to the employee's success in preventing data loss events

Training cannot be delivered once or twice a year in the form of quizzes or videos; it must be embedded into daily workflows to truly have an impact

Training should give more to our organisation than a tick in the box on the matter of compliance; it should enforce a security culture powered by insights into employee behaviour

Chapter 5:

The risks, roles and limitations of AI and LLM

Liam Cahill
Founder and Advisor to national bodies, local providers and healthtech companies

As with virtually every other sector, the cybersecurity world is responding to the explosive advancement of generative AI including, but not limited to, Large Language Models (LLMs).

Many of us have tried a range of these tools and considered how and whether they should be deployed in our organisations. In McKinsey's "The state of AI in 2023: Generative AI's breakout year," 79% of respondents say they've had some exposure to generative AI and 22% say they are regularly using it in their own work.

What constitutes the ethical use of AI, such as content used in citizen-facing interactions by public services, or technology to automate opinions, analysis and perspectives, is also under consideration. Indeed, the ethical and legal use of AI driven technologies will shape the development of new and existing data protection regulations with privacy lawyers quick to emphasise that AI developers engaging in web scraping and analytics must comply with the GDPR.

While organisations across all sectors are considering the opportunities of AI, so too are cyber-criminals, with 'threat actors' using LLM to rapidly produce more sophisticated, convincing, personalised and prolific scams.

Unsurprisingly, cyber security agencies and advisors are putting this at the forefront of their education and recommendations for public and private sector organisations alike. The UK's National Cyber Security Centre (NCSC), run by GCHQ, stated in their seventh annual review:

"In the short term, AI technology is more likely to amplify existing cyber threats than create wholly new ones but it will almost certainly sharply increase the speed and scale of some attacks."

Fight fire with fire

One vector most vulnerable to the risks of generative AI and social engineering attacks is email. Enhancing security measures in email to enable employees to identify and report on potential threats should be top of mind for businesses next year. Naturally, this relies on employee awareness, and arming users with appropriate tools to manage risk.

Adopting a secure by design stance in the implementation of any and all new technologies can protect organisations against the threat of AI. Guidelines developed by the NCSC, US Cybersecurity and Infrastructure Security Agency (CISA), and 21 other international agencies, detail guidance for providers of any systems that use AI to:

"Build systems that function as intended, are available when needed, and work without revealing sensitive data to unauthorised parties."

Leveraging smart technologies can protect your organisation against malicious social engineering attacks. So, in addition to confirmation of vendor certifications, understanding your security provider's use of AI should now be part and parcel of any provider audit. Many organisations now claim to utilize AI and machine learning – but what is their experience and expertise?

Investigating their track record in the form of customer testimonials and case studies will contribute to your understanding of their product and capabilities for your specific requirements.

In addition, relying solely on AI to manage risk is not a failsafe measure. While AI can be very efficient at identifying cybersecurity threats, it is vital that the right people are involved in managing relevant procedures and platforms. 2024 should see the introduction of AI governance policies, ensuring the people on the frontline of the most vulnerable systems and networks are prepared with the knowledge required to prevent potential attacks.

Key takeaways:

AI, LLM and machine learning technology present great opportunities for efficiency and security

Work with suppliers to understand their approach to AI, including how they manage data protection under the GDPR and other regulations

AI and people are stronger together. Relying solely on AI to prevent attacks is unwise.

zivver

London

5 New Street Square
EC4A 3TW London
United Kingdom

+44 (0) 203 285 6300

Amsterdam

Spaklerweg 52
1114AE Amsterdam
The Netherlands

+31 (0) 85 01 60 555