INDEPENDENT PUBLICATION BY

Raconteur

RACONTEUR.NET | #0874 | 25/06/2023

CYBERSECURITY & AUTHENTICATION

REGULATION

Cyber house rules: how Brussels is setting an identification standard

The EU's new digital identity framework, EIDAS 2.0, could spur similar regulatory initiatives elsewhere. While the UK is likely to take a different path, excessive divergence would not be ideal

Ben Edwards

Brussels has moved to strengthen its legislative clampdown on cybercrime in recent months by means of the revamped electronic identification, authentication and trust services regulation (EIDAS 2.0). This measure is designed to grant at least 80% of EU citizens a digital ID wallet by 2030.

The legislation should pass the trialogue discussions held by the European Commission, Parliament and Council over the next couple of months, after which a transitional period will be in place for member states to set up their own processes for approving digital wallets.

So says Andrew Bud, founder and CEO of iProov, a specialist in biometric authentication and ID verification. "In terms of implementation, we are approaching the end of the beginning," he reports.

Significant wrinkles still need to be ironed out. For starters, some existing (and successful) national programmes – Italy's Sistema Pubblico di identità Digitale, for instance, which has almost 35 million active users – fall short of the highest level of verification assurance required by the new regulation.

"None of those users would be considered adequately onboarded, so they would need to go through that process all over again to qualify for EIDAS 2.0 identities," Bud says.

While the EU is working to limit such disruption, the task of developing the technical standards required to meet the highest levels of assurance is not straightforward.

"The underlying standards – W3C verifiable credentials – are evolving, so it is tricky to build upon a moving foundation," Bud explains.

> **The brutal reality that people must understand is that it's not *if* their identity is going to be compromised; it's *when***

This all means that numerous unanswered questions remain about how the EIDAS 2.0 framework will work in practice.

Neil Slater is regional director, UK and Ireland, at Veridas, a Spanish firm specialising in biometric ID systems. He believes that there is "a significant challenge as to what the commercial model is going to look like and who is going to be responsible for the data. There are still many things that need to be resolved. How will the people who provide that digital identity be compensated, for instance?"

Despite such uncertainty, most market watchers believe that EIDAS 2.0 will turn out to be a game-changer for digital ID schemes more broadly.

"This will disrupt the way digital identity is done worldwide," Bud predicts. "The European digital identity wallet will be the first large international scheme to be based on verifiable credential technology. Until now, verifiable credentials have been a far-off aspiration for technologists. Adoption by the EU changes everything. It will lead to the adoption of this tech elsewhere."

Westminster is taking a different tack from that of Brussels by seeking to introduce a framework that gives private sector providers more leeway in how they develop solutions, as long as these meet certain baseline criteria. That's the view of Will Richmond-Coggan, a partner specialising in data privacy at law firm Freeths.

"It will be interesting to see whether the European approach – a top-down diktat about exactly what the verification technology needs to comprise – will turn out to be more successful than the more flexible approach we are likely to see from the UK," he says.

Richmond-Coggan adds that the need for a more harmonised set of global standards will become increasingly important as more countries develop digital ID schemes of their own.

"What drives EIDAS 2.0 is the recognition that digital identity verification is meaningless if it's not transnational, given that so much commerce is cross-border in nature," he says. "If you are validating someone's identity, you need that to be recognised consistently wherever you are in the world."

As the development of digital ID schemes gathers momentum globally, some analysts have voiced concerns that a significant proportion of this work could slip into the hands of big tech. The fear is that such an outcome could restrict innovation.

"Control of digital identity data is extremely commercially valuable to platform operators whose revenues depend on advertising or the monetisation of access to their platform users," Bud explains. "The bigger players, which can more easily add identity data to their collection of revenue-generating services, will create barriers to those seeking to develop competitive alternatives."

To deal with that risk, the EU has been enacting policies designed to ensure that innovation and competition continue unimpeded. For instance, the Digital Markets Act 2022 protects third-party identity service providers from incurring additional charges from big tech when accessing devices to verify users.

The recent advances in generative AI may also focus minds on the need for wider digital ID adoption to reduce the risk of online fraud, Bud notes.

"The ability to create sophisticated fake images and voices – and, indeed, conversations – has become available to almost everyone," he says. "We will soon be unable to tell the difference between a fake image and a human being."

This means that ID verification tech will need to incorporate so-called liveness detection systems. These are designed to ensure there is a real person involved and not computer-generated imagery.

Past ID initiatives have generally elicited either resistance or apathy from British consumers. With this in mind, a public education programme may soon be appropriate, according to Slater.

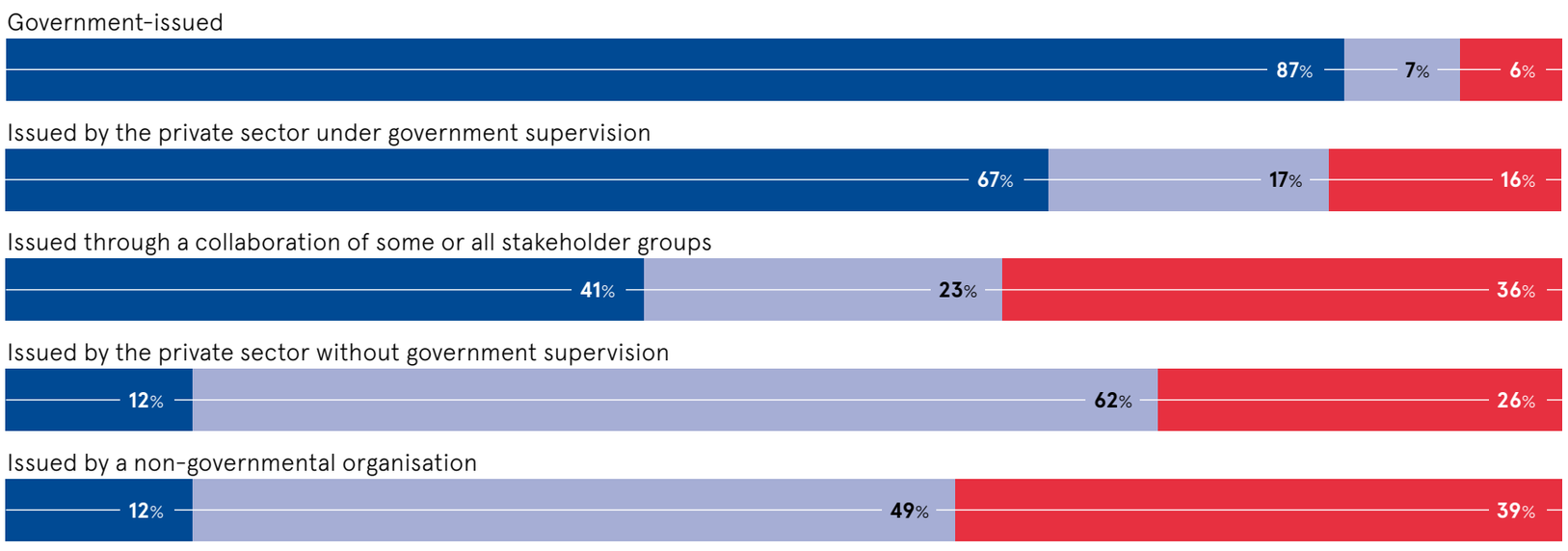
"We need to start really educating people on the benefits of having a digital identity and explaining that it isn't one step closer to giving Big Brother control over our lives," he says. "The brutal reality that people must understand is that it's not *if* their identity is going to be compromised; it's *when* – and that a digital ID can add a significant layer of security."

Bud believes that the prospects for digital ID are brighter in the UK than they have been at any time over the past decade, but he notes that challenges remain. The lack of a clear approach from policy-makers is a risk, he says, and the government has yet to map out how AI, privacy and cybersecurity regulation will work together.

"Lots of important plates are spinning just now," Bud says. "It's crucial that not one of them breaks."

GOVERNMENT-ISSUED DIGITAL IDENTITY VERIFICATION SYSTEMS ARE GENERALLY HIGHLY TRUSTED WORLDWIDE

Consumers' responses when asked about the trustworthiness of digital IDs issued in the following ways



Association of Certified Anti-Money Laundering Specialists, Royal United Services Institute, YouGov, 2021

Distributed in
THE SUNDAY TIMES

Contributors

Jon Axworthy
A journalist specialising in healthcare, science, technology and the future.

Ben Edwards
A freelance journalist who specialises in finance, business, law and technology.

Christine Horton
A long-time contributor to specialist IT titles, writing about technology's impact on business.

Tamlin Magee
A London-based freelance journalist specialising in technology and culture.

Charles Orton-Jones
A former Professional Publishers Association Business Journalist of the Year who specialises in covering fintech and startups.

Emma Woollacott
A business, science and technology journalist with more than two decades of experience.

Raconteur

Campaign manager
Alfie Turnell

Reports editor
Ian Deering

Deputy reports editor
James Sutton

Editor
Sarah Vizard

Chief sub-editor
Neil Cole

Sub-editor
Christina Ryder

Commercial content editors
Laura Bithell
Joy Persaud

Associate commercial editor
Phoebe Borwell

Head of production
Justyna O'Connell

Production executive
Sabrina Severino

Design
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Sean Wyatt-Livesley

Illustration
Sara Gelfgren
Kellie Jerrard

Design director
Tim Whitlock

raconteur-media
@raconteur
@raconteur.stories

raconteur.net /cybersecurity-2023

Commercial feature

Digital resilience: how firms can build a team approach

How can security teams become proactive when it comes to managing risk – and work collaboratively across a business? Five experts discussed these topics and more at a recent roundtable

A cyberattack is probably one of the worst nightmares a company can face, especially as digital systems evolve, data proliferates and technology advances at pace. Business can be interrupted, consumers' information can be compromised, and reputations can suffer – and managing risks is arguably more complicated than ever.

The challenges for security professionals are many and varied, including how the risk of an incident is presented to board directors and ways in which buy-in and budgets can be secured.

For Tony Burton, managing director for cyber and trust at consulting and manufacturing firm Thales, one of the toughest questions to answer is how resilient is resilient enough – and how do you measure it?

"If you go through the cycle of detecting [an incident], finding something, doing something about it, trying to respond, there's an impact to the business and you can see that it's tangible," he says. But resilience is a product of many variables, including the training people have and how often tools are updated, he adds.

"All of which need a level of investment, which ultimately boards need to sign up to," Burton says.

Key challenges

For James Humbles, head of IT governance and risk at credit company Novuna, these tough board conversations are starting to happen, especially in the face of financial services regulation. "This is the level of risk your company is exposed to, is that acceptable? Is that within tolerance, or do you need to spend some money, or do you need us to find a ... different solution?" are some of the questions being discussed, he says.

Getting the investment right is a balance, according to Mark Woods, chief technical adviser, EMEA, at enterprise resilience platform Splunk. "When it comes to systems, I talk about stability, responsiveness, and predictability and you can't have them all. Normally, when you make a big investment, are you making that investment for stability or responsiveness? Often, the focus is not made clear. Typically, you surround that with something that is going to give you a level of predictability," he says.

Richard Frost, chief information security officer at insurance firm Esure, puts in place key risk indicators (KRIs) and key performance indicators (KPIs) which he discusses with the company's risk committee every month. But what he finds challenging is the thousands of vulnerabilities in the cloud – Esure is in the middle of a digital transformation – and working out how to prioritise them.

"Security should be proactive, where we should be secure enough to allow the business to disrupt the market ... what that means is we need to have the best security controls possible – which means big investment," Frost says.

Future proofing

Long-term business strategies also require a proactive approach to security. Dunnhumby, the data organisation owned by Tesco, is about six months into a three-year plan, and the company's chief information and security officer Martyn Booth is working on getting the security team ready for that time when the risk profile will "dramatically shift."

"Strategically [we are working on] understanding where the business is going and what they need from us when, so that we can prepare backwards in terms of budgets... and getting buy-in from the relevant stakeholders," he says.

In many industries, technology is evolving at pace, and sometimes blending – as is the case in the automotive and energy sectors, which are working together on infrastructure for electric vehicles (EVs).

The UK's ambition to stop production of cars with combustion engines by 2030 will require innovative ways to make sure there is enough electricity for these new EVs. "The real challenge is in the information that allows all of that to happen – it has to be accurate and dependable," Burton says.

> **A real challenge in the UK is access to all of the right level and volume of skills to be able to deal with ... everything from cybersecurity through to the broader resilience [of a business]**

In the face of competition from outside nations and even potential organised crime, the threat landscape needs to be considered early on, he adds.

Esure's Frost aims to get senior executives involved in projects early so they understand what's required from a security perspective – and how much it might cost. "I've been in situations at other companies where all of a sudden, security comes in at the last minute and says: 'this isn't good enough,' and that can cause friction," he says. Frost now has security architecture reporting to him, as well as having development security operations engineers, so that he can "embed" security into different teams, he says.

Business culture and teams

Having teams from different disciplines work well together is something many of the panel are grappling with. Dunnhumby has around 1,200 developers, and one challenge is having technology teams embed common ways of working, says Booth.

"We just can't, as a security team, be expected to hook into that many different ways of working and have a flexible enough process that will cater for effectively 700 or so different ways of doing the same thing," he says.

Making sure security is consistent in its application is also a challenge for Dunnhumby. "It involves lots of soft stuff that we're not as good at as security professionals – like cultural change – we're trying to work out how to crack that," Booth says.

Collaboration is important for Humbles at Novuna, who spends a lot of time with the organisation's security architect, who reports to the chief technology officer, as well as the head of information security, to make sure their activities are aligned. "We make sure that the [people on the] projects know their boundaries and how far they can go before they need to come and do a sense check," he says.

One of the challenges when talking about resilience and security threats is that most people within a business are not experts. Woods points out, and they may not engage with documentation about risk profiles, because it's intimidating, or people feel they don't have time to understand it. He suggests trying to communicate in plain English what assumptions are being made by the business and visibly show how this contributes to a resilience risk.

Skills challenge

Another issue the panel brings up is a shortage of talent. "A real challenge in the UK is access to all of the right level and volume of skills to be able to deal with ... everything from cybersecurity through to the broader resilience [of a business]," Burton says.

For Woods, being honest about the impact someone may have in an organisation is the best policy. Technically astute people, "who could go pretty much anywhere," will see through corporate-speak about a company's purpose, he says. "Be really specific about the things that they need [to do the job], and the things that you'll train them on," he suggests.

Other participants advocate apprenticeship schemes, with Novuna having apprentices working across various IT functions. "The sooner we get them, and get them engaged, the better they become," he says.

And Frost's approach is to give people what they want. "If you go through a transformation, you've got new, interesting work – and people love those things."

The challenges for security teams are coming fast and furious, and alongside providing interesting work for teams, they're set to keep firms busy for the foreseeable future. But the strategies for success are clear: work with senior leaders to help them understand what's important early on, focus on a collaborative culture – and one that communicates well across teams – and work hard to attract new entrants. And – be sure to speak in plain English.

RISK MANAGEMENT

What happens if cyber insurance becomes unviable?

Although insurers are innovating furiously to keep their products affordable, they're running short of options. The problem is becoming so serious that government intervention could soon be required

Craig Whitehead via Unsplash

Emma Woollacott

The average global cost of a successful cyber attack hit a new high of $4.35m (£3.41m) last year, according to IBM's latest *Cost of a Data Breach Report*. And that's not the end of the bad news: research aggregator Statista has forecast that the global cost of cybercrime will double within the next four years to $23.8tn.

Not surprisingly, the cost of insuring businesses against this risk has been rocketing as well. Insurance broker Marsh has reported that premiums for cybercrime cover leapt by 28% in Q4 2022 and another 11% in the following quarter.

There have even been suggestions that cyber insurance is becoming unsustainable. Huntsman Security, for instance, has predicted that the number of firms that will be unable to afford premiums or be declined insurance (or face significant cover limitations) will double year on year in 2023. And the Federation of European Risk Management Associations (Ferma) warned late last year that cyber insurance was in danger of becoming "an unviable product".

Ferma's CEO, Typhaine Beaupérin, says that, "spurred on by a growing understanding of the risk landscape and a spike in claims, the cyber insurance market has experienced a period of significant rate hardening and a narrowing of the scope of cover in recent years, as more stringent conditions and exclusions are applied".

For most organisations, discontinuing cyber cover isn't an option, because such insurance is often a standard requirement in requests for proposals.

As a result, insurers are adapting their offerings to keep the boat afloat. Many are trying to maintain affordability by altering their policies to restrict the types of incidents they will cover. For instance, Lloyd's of London will no longer indemnify organisations against losses from nation-state cyber attacks or those taking place during wars. Chubb has proposed a broad hacking exclusion and insurance deductibles for certain large-scale hacks, while Beazley has excluded catastrophic events, making war insurance a separate product.

Insurers have had to "learn quickly and continue to iterate on offerings, coverage and approaches to assess cyber risk and policy language", says Heidi Shey, principal analyst, security and risk, at Forrester. "We have seen a push for standalone policies with much clearer language about what is and what isn't covered. And we've seen the introduction of new war exclusion clauses that specifically address cyber attacks."

Some insurers are trying to keep their policies affordable by requiring ever-stronger security practices from their clients, reports Anthony Cordonnier, MD at risk and reinsurance company Guy Carpenter.

"Given the heightened risk landscape, underwriters are exercising a stronger level of technical acumen than ever before," he says. "There are higher security hurdles to clear in order to secure cover."

As a result, controls such as regular patching and the use of multi-factor authentication are considered "industry table stakes", Cordonnier adds.

New deals are emerging for SMEs, with insurers offering them more affordable cover alongside risk monitoring and alerting solutions or cybersecurity-related offerings. These can include virtual CISO services; security training and awareness resources; risk assessments; and monitoring and managed services.

Paul Handy is global head of cyber risks at Crawford & Company, a specialist in claims management. He reports that "insurance carriers have introduced managed risk solutions for SMEs in which they engage with customers throughout the policy term to manage any potential exposures. We have been seeing some innovative solutions, such as defined benefit policies for cyber business interruption, parametric coverage and limited coverage and co-insurance clauses for ransomware risk. These are all new ways of managing overall risk and exposure, making things sustainable from a claims management perspective."

Also emerging are product-specific partnerships, such as AIG's CyberMatics model, offered alongside support from security tech providers, and the Cloud Protection + solution that Munich Re and Allianz are marketing to Google Cloud users.

> **Businesses and the insurance market cannot be expected to carry this burden alone**

Despite such innovations, there is widespread concern that the industry's efforts still won't be sufficient. This has prompted some governments to consider intervening. The US Treasury, for example, is exploring the idea of a federal insurance response to catastrophic cyber events, possibly on the condition that organisations adopt certain minimum security standards.

There have been calls for a similar scheme in Australia, while talks are taking place in the UK between insurers and the government about a possible expansion of the Pool Re terrorism reinsurance scheme. This was introduced in 1993, when insurers stopped offering coverage against acts of terrorism after a string of bombings by the Provisional Irish Republican Army. Insurers are hoping that it could be extended to cover state-sponsored or war-related cyber attacks.

"Ferma firmly believes that collaboration is needed to address the systemic potential of cyber risk. Businesses and the insurance market cannot be expected to carry the burden alone," Beaupérin says. "If we are to manage the scale of the threat posed by systemic cyber risk, we need collective action that combines insurer capacity and expertise with public sector funding in the form of public-private partnerships."

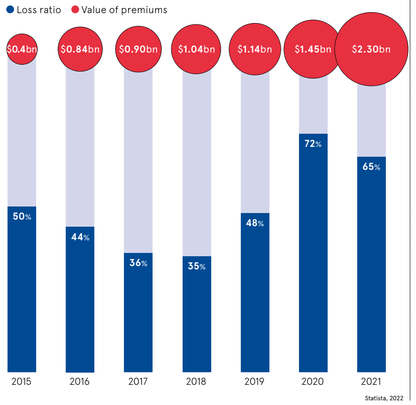
Ferma also favours a concerted international initiative to tackle digital risks that would run along similar lines to the United Nations' COP climate conventions. Key issues for discussion could include systemic risk; public-private partnerships and state backstops; and security standards.

For Beaupérin, the bottom line is that no stakeholder can afford to let cyber insurance become unviable.

"At this critical stage", he says, "greater cooperation is central to maintaining a sector that meets the risk needs of both insurers and policy-holders." ●

PREMIUMS ARE ON THE RISE – AS ARE LOSSES TO CYBER INSURERS

Total value of premiums earned and loss ratio (direct losses plus defence costs divided by premiums earned) for standalone cyber insurance policies in the US from 2015 to 2021



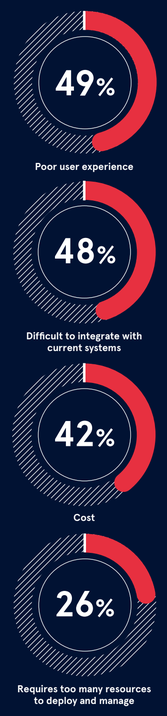
Statista, 2022

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) refers to any method of authentication in which a user is granted access to a point only once they have provided at least two items of identifying evidence. MFA is one of the most common user-access techniques used by businesses to defend against cyber attacks. But how effective is this approach? And, as cybercriminals constantly adapt their tactics and probe for weaknesses, how can it be enhanced?

OBSTACLES TO MFA DEPLOYMENT

Share of tech professionals citing the following as obstacles to traditional MFA adoption



Cybersecurity Insiders, 2022

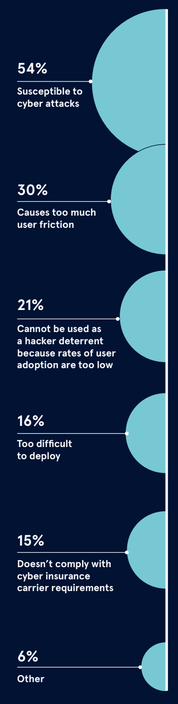
MOST COMPANIES ARE PRIORITISING SOME TYPE OF MFA

SecureAuth, 2023

Share of business decision-makers citing the following measures as priorities for 2023

THE WEAKNESSES OF TRADITIONAL MFA

Share of decision-makers agreeing with the following negative statements about traditional MFA

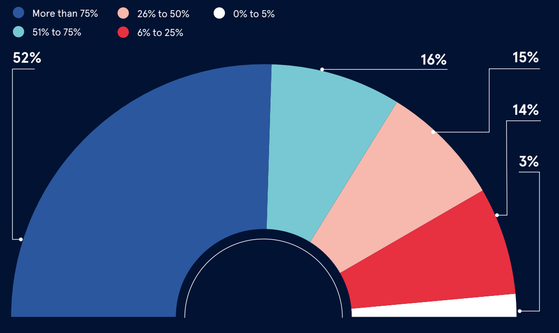


SecureAuth, 2023

THE USE OF TRADITIONAL MFA ACROSS ORGANISATIONS

SecureAuth, 2023

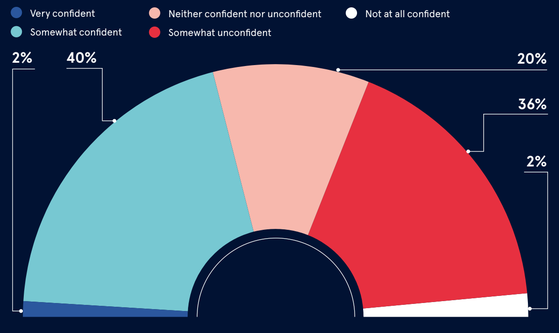
Share of decision-makers giving the following responses when asked to cite the extent of MFA coverage in their firms



IS TRADITIONAL MFA ENOUGH TO WARD OFF ATTACKS?

SecureAuth, 2023

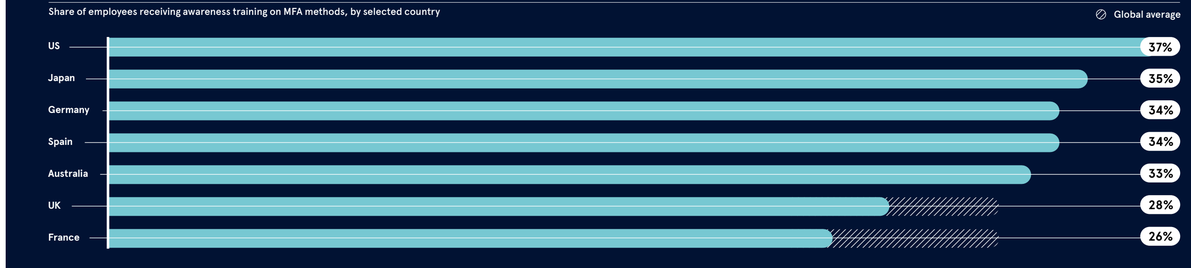
Share of decision-makers giving the following responses when asked how confident they were in traditional MFA



THE UK FALLS BELOW THE GLOBAL AVERAGE IN MFA EDUCATION

Proofpoint, 2022

Share of employees receiving awareness training on MFA methods, by selected country



EDUCATION

The kids aren't alright

Even though generation Z is the first to have been raised by the internet, its members are relatively weak on cybersecurity. They're not totally to blame for that, though

Tamlin Magee

As the big economies of the West boomed after the second world war, adolescents in those countries, especially the US, gained significant spending power for the first time. This prompted businesses to create a whole new marketing segment for them, putting the term 'teenager' into common usage. By the 1970s, the generation gap had come into play: it was no longer about how old you were, but when you were born. Such slicing and dicing has since evolved into a system featuring several age categories, including the silent generation, post-war baby boomers, generation X and millennials. Today's teens and under-25s are known collectively as gen Z, while those born since the early 2010s are classed as gen alpha.

If you type gen Z's other name, 'zoomers', into your favoured internet search engine, you'll find all sorts of claims about their characteristics, many of which are contradictory. They're political activists, yet they're nihilists. They're into trends such as urban fishing, but they're also hard-nosed capitalists. Apparently, they cannot abide millennials, punctuation or the US.

Whether such sweeping generalisations could possibly hold true for the world's 2 billion zoomers is beside the point. The one key factor that unifies them all is that they are the primordial internet-brained batch, the first that has only ever known life with the net seeping into every pore, for better or for worse. For many of them, using a smartphone is as natural as drawing breath. They spend half of their waking lives looking at a screen, according to research published last year by the *Los Angeles Times*.

Yet, for all their familiarity with the digital world, significant problems have arisen for zoomers as they've entered the workplace and been confronted by antediluvian hardware and software. Reports abound of gen Z's struggles with office tech such as printers and spreadsheets.

A general IT literacy gap may exist, then, but more worrying than a junior employee's inability to work a photocopier is the potential cybersecurity threat this gap presents. A survey conducted last year by the National Cybersecurity Alliance made some surprising findings. It found that, despite their close acquaintance with the digital economy, 64% of zoomers did not rate cybersecurity as a high priority. They also reported a higher cybercrime victimisation rate than other age groups and were most likely to take phishing bait.

During the depths of the Covid crisis, younger employees also experienced more IT problems than their older colleagues while working remotely. According to a survey by *Security* magazine, 38% of zoomers were logging four or more tech-related issues a week on average in Q2 2020, compared with 12% of colleagues aged 45 to 54. Zoomers engage in riskier behaviour too: although they do understand the need to change their passwords regularly, they don't actually do so, according to the World Economic Forum.

Gen Z's apparent lack of computer literacy and lax attitude to cybersecurity may spell trouble for everyone. The digital economy has become even more interlinked in nature since the Covid crisis, when millions of people were obliged to live more of their lives on the internet. Critical infrastructure, medical records, personal data – it's all online. The recent upsurge in supply chain attacks shows that criminals need find only one defensive weak link to cause widespread damage. Consider a hospital to which an employee accidentally introduces ransomware, effectively shutting down its vital systems – literally a matter of life and death.

All this seems a little mystifying, given that gen Z has widely been touted as the most IT-savvy generation. But the 'digital native' badge is possibly an unhelpful one, according to Dr Elinor Carmi, lecturer in data politics and social justice at City, University of London. She observes that, while people are indeed becoming acquainted with online tech at a younger and younger age, the range of applications they're using is actually quite limited.

"When I ask my students what they mean when they say they're online, 99% tell me that they mean they're using TikTok," Carmi reports. "If you're experiencing only one thing, that limits how you understand different types of options and what's available to you."

Researchers at Royal Holloway, University of London, are studying the apparent contradiction between zoomers' comfort with digital tech and their risky behaviour online. Some of the answers might lie in human biology, suggests Professor Dawn Watling, director of the college's social development lab.

The prefrontal cortex, which helps us to make rational decisions and exercise cognitive control, is one of the last parts of the brain to mature, she says. By contrast, the limbic system – which contains areas of the brain involved in reward and reinforcement – develops sooner, so it may be more natural for younger people to, say, open a dodgy email promising a huge cash windfall.

> **If you have an individual who doesn't care much about their own data, what attention are they going to pay to their organisation's data?**

> **When we use solely technical terms, that puts people off. Our messaging has to change: we must cover the reality of personal outcomes and use real-life examples**

At the same time, zoomers may have developed a sense of complacency that they are less likely than older people to become cybercrime victims simply because they've grown up with digital tech.

"On top of such overconfidence, there's been a lack of understanding about the consequences," says Watling's colleague, Dr Konstantinos Mersinas, director of Royal Holloway's distance-learning programme in information security. "They might say: 'OK, maybe my phone is hacked, but I'll survive.' Such an attitude is related to risk-seeking behaviour. If you have an individual who doesn't care much about their own data, what attention are they going to pay to their organisation's data?"

Yet apathy is not the predominant attitude that Lisa Plaggemier, executive director of the National Cybersecurity Alliance, has detected in her conversations with zoomers. Rather, it's a prevailing sense of nihilism tied to their perceived lack of agency. Contrary to what many people might think, gen Z is mistrustful of the tech sector, according to research by marketing agency FleishmanHillard in 2020, yet many feel powerless against the might of big tech. Having grown up with the internet and learnt of many high-profile data breaches, they feel that "the horse is out of the barn and there's not a lot they can do", Plaggemier says.

That's not actually true, she adds, but cybersecurity has such an image problem that the effective safeguards that zoomers could apply are often ignored.

If this situation persists, the cyber literacy gap could become a chasm, prompting criminals to subject their always-online young quarry to a constant bombardment.

A big problem here is the perception that effective cyber hygiene is an onerous chore. This misapprehension needs to be tackled socially, starting at school, according to Mark Brown, MD for digital trust at the British Standards Institution (BSI).

"We often talk about cybersecurity from a deep technical perspective, but what we haven't discussed is its societal impact in a non-technical way," he says. "When we use solely technical terms, that puts people off. Our messaging has to change: we must cover the reality of personal outcomes and use real-life examples."

Carmi suggests that one way to prepare young people better could be for schools to focus more on teaching critical thinking skills. She notes that, while data literacy is mentioned in the continuing saga that is the UK's online safety bill, regulators are understandably reluctant to take ownership of such a project.

"It's not something you can do really quickly, but governments prefer to think about the moment rather than the future," Carmi says. "We need a future thinking programme for different demographic groups who haven't learnt this in schools and universities. It needs to provide ongoing support, because things learnt five years ago may not be relevant today. But some factors are never going to change – teaching people how to cross-check sources will still be relevant in 10 years' time, for instance. And core skills such as assessing whether websites (or people) are legitimate or not are important."

There are signs that some of tech's biggest players are starting to position factors such as data privacy as a competitive differentiator. Apple's recent advert featuring US comedian Jane Lynch, for instance, may go some way towards addressing cybersecurity's image problem.

More could be done, though. Plaggemier says that, if she could be granted one wish, it would be for businesses to use multi-factor authentication as the default, providing a huge security boost at a stroke.

But finding a solution to the problem won't be simple. It will require a concerted effort from government and the tech sector to communicate in clear terms why security is important. They must collaborate to explain the benefits of good cyber hygiene and provide ongoing support for users of all ages, taking into account not only the technology but also the psychology involved.

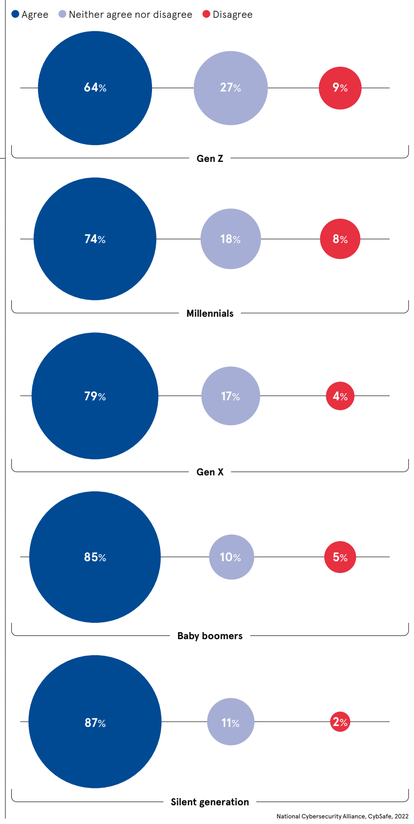
This issue cannot be attributed to some inherent generational difference. There's strong evidence to suggest that the rest of us have let a generational cyber literacy gap widen too far. Where governments have run awareness campaigns, these have changed people's views and habits. Take the UAE, for example: one of the world's most digitally advanced economies has used a targeted public education programme to make cybersecurity a key concern among younger people.

Traditional training will not work in this context and neither will sanctions, according to Watling and Mersinas.

"If it's too disruptive to people's work, they often seek alternative ways to do what they want to do," Watling argues. "We think it's crucial to consider cybersecurity culture, how we explain things to people and how we support their own buy-in. Training is important, but we need to think more generally about what kind of cybersecurity culture we have." ●

GEN Z IS THE GENERATION LEAST LIKELY TO PRIORITISE CYBERSECURITY

Internet users' level of agreement that staying secure online is a priority, by generation



National Cybersecurity Alliance, CybSafe, 2022

drnedg via iStock

Uncle Sam's change of stance on cybersecurity

In March, Joe Biden's government published a national cybersecurity strategy stating in no uncertain terms that self-regulation had failed.

The document argued that "continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience". It added that businesses would need to take a more proactive approach in this area, which could include hiring ethical hackers to test their defences.

But does this change of onus risk further undermining people's sense of individual responsibility, especially when many feel that they lack agency as it is?

The BSI's Mark Brown doesn't think so. In fact, he says, this measure has been "a long time coming. While the US is seen as a forerunner in the advancement of technological progress, the legislative leaders have probably been the EU and the UK. If we go back to 2007-08, when the General Data Protection Regulation became an idea, it was for exactly the same reasons. There had been several massive data breaches across the continent. Market forces and voluntary conditions were seen not to be working. The fines in place for breaches of data privacy and cybersecurity meant little to nearly all organisations, so it was recognised that something had to be done."

The US national cybersecurity strategy actually "emphasises the need for those best suited to mitigate security risks to do so", says Zeki Turedi, field CTO, Europe, at cybersecurity specialist CrowdStrike.

He observes that the mandate for agencies to use modern cybersecurity technologies and best practices such as zero-trust architecture, threat hunting and log management is a step that other countries could adopt in tandem. This would help to set a new standard for what reasonable security looks like.

But governments and big tech are at odds here, which could present unintended ramifications for the rest of us. The UK's online safety bill aimed to blunt the powers of big tech, or at least force the sector to take more responsibility, notes Konstantinos Mersinas at Royal Holloway.

"But where this story goes is that the bill is going to undermine the individual's privacy at the end of the day," he says. "The government seems to be fine with that, although it's not stated like this in public."

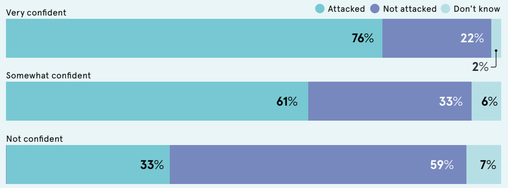
Ultimately, people will still need to play a key role in keeping themselves safe online. After all, while organisations would rightly be fined for leaking credit card data, it's also up to the individual not to do something as foolish as publishing such information themselves.

"I don't think security can be forced. It doesn't work like that," says Mersinas, who adds that organisations will need to start considering a range of measures. "I think you have to take several strategic approaches to enhance your overall security culture. For most organisations, that will include a positive framing, so that people realise the risks and individually embrace actions that expand to their colleagues, their department and then the wider company. But it's not an easy answer."

Commercial feature

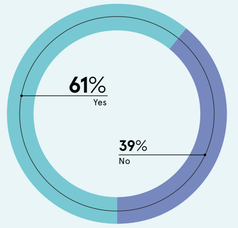
CONFIDENCE CORRELATES WITH YOUR ODDS OF HAVING SUFFERED AN ATTACK

Cybersecurity professionals' confidence about defending their organisation in future, by whether or not they have suffered an attack in the past two years



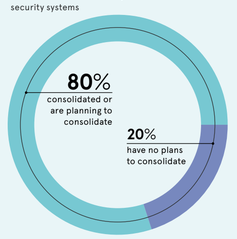
FRAGMENTATION IS SEEN AS A BARRIER TO IMPROVING RESILIENCE

% of cybersecurity professionals who agree that the complexity of the market is holding back progress



TECH CONSOLIDATION IS ONE POSSIBLE SOLUTION

% of cybersecurity professionals who plan to consolidate or have already consolidated their security systems



Is cybersecurity overconfidence causing complacency?

Cybersecurity is moving up the boardroom agenda, but implementing solutions too quickly can result in a confusing mix of tools across your infrastructure, leading to a sense of being more protected than you are

Cybersecurity is a key topic for discussion in boardrooms everywhere – with its critical importance to daily operations, growth and revenue rapidly moving it up the CEO and C-suite agenda.

Making sure your organisation is resilient to ever-changing threats must remain a top priority, with CISOs given the directive to protect the business and its strategic objectives. A successful breach could cause costly downtime, reputational damage, the loss of sensitive information and, ultimately, huge financial loss.

John Maynard is CEO of Adarma, one of the largest independent cybersecurity services companies in the UK and which runs security operations for many of the FTSE 350. He warns that there is no room for complacency in developing and implementing a successful cybersecurity strategy.

"Our recent research found 53% of the 500 senior cybersecurity professionals it questioned were 'very confident' they did not have gaps in their control's coverage, with 42% 'somewhat confident'.

"However, three-quarters of those who were 'very confident' had been breached in the past two years, while a third of those who were 'not confident' had suffered a breach," he says.

All respondents to the Adarma survey were from organisations with 2,000+ employees, and Maynard adds: "We found the more confident security teams are, the more likely they are to have suffered a breach in the past two years. The danger is that this misplaced confidence will lead to complacency, putting the organisation at greater risk of attack."

A fragmented market of tools

Another finding from the research was how many believe the cybersecurity market is fragmented, complex and cluttered when it comes to the solutions offered. Six in 10 suggested this is now a barrier to improving their capability and performance in security.

This is exemplified by the UK government's cybersecurity sectoral analysis from 2022, which shows 1,838 firms are active within the market, providing cybersecurity products and services.

Additionally, says Maynard, a wide range of acronyms is adding to the confusion, leading companies to potentially misunderstand or overestimate the capabilities of their security technology.

"Our IT environments have become hugely complex and expansive over recent years. As organisations have moved to the cloud, many have enabled a largely remote workforce and so the attack surface has grown," he explains.

"Security teams have generally been acquiring technology to try to keep pace with this change and the threat posed by adversaries, but they find themselves in a very complicated place with a patchwork of tools either overlapping in capability or presenting gaps."

With organisations having now acquired a large number of security tools, Dan Baker, chief delivery officer at Adarma, points out the risk. "As the security technology landscape has matured and expanded, this has become one pitfall to be wary of," he says. "Unless an organisation has the capability and resource to feed, water and integrate these tools, they can provide an unrealistic safety blanket."

Scott McElney, global chief information security officer at the Weir Group, agrees and warns: "Having more tools doesn't mean you're more secure. It could add more risk if you don't have the expertise to fine-tune and harmonise them across your digital ecosystem."

> **Organisations need to take a holistic approach that combines people, process and technology, but this can be challenging in a market where cyber talent is in short supply and many businesses have conflicting priorities**

Piling the pressure on CISOs

With CISOs under considerable strain, it's no wonder that security teams can be tempted to adopt the newest cutting-edge tools that claim to be the next cybersecurity silver bullet, says Maynard. It's a problem that chimes with Adarma's research.

"We can't rely solely on technology to solve our cybersecurity problems," he explains. "Organisations need to take a holistic approach that combines people, process and technology, but this can be challenging in a market where cyber talent is in short supply and many businesses have conflicting priorities."

He suggests effective cybersecurity planning is a "marathon not a sprint", explaining how security teams should not mark their own homework. Instead, the better option, says Maynard, is to engage an independent party to challenge security posture and enable "the ongoing development of resilience".

Adarma's findings also showed how eight in 10 security teams have, or plan to, consolidate their security tooling; Maynard suggests it is vital that people "run the technology, rather than the technology running itself".

He adds: "It's critical you have the right engineering and analyst resources working to configure and optimise your tools, so you are defending against the threats that matter to your business."

Baker also explains how many of Adarma's customers are looking to consolidate and simplify their technology stack. But he suggests to do so they must first gain a better understanding of what to consolidate and the value it presents. However, while the bottom line is often a driver for such a move, Baker warns: "Security teams must ensure they don't jeopardise their cyber resilience in the process."

Taking a people-first approach

According to the Weir Group's McElney, a skilled security architect should lead this sort of project, sponsored by the CISO. "When you look at changing your security tooling, there are lots of interested parties who are motivated by different needs, so a consolidation project needs to be led by someone independent, like an architect," he says.

Maynard adds: "If you can consolidate your tools and get greater visibility over your application estate, you will be able to resource more effectively, reduce digital fragmentation and create more centralised competencies. That will enable your security team to focus on getting the best out of the products you have."

There is another challenge to be overcome: the state of vendor lock-in or fears over losing functionality and flexibility. A technology-agnostic and hybrid approach to security can help reduce the risk of becoming too dependent on a single provider, while working with a trusted security partner that prioritises interoperability and takes a holistic view of security can help avoid a state of dependency.

"We can't rely solely on technology to make our organisations resilient. Security teams need a set of tools that they have the expertise to manage, configure and optimise. Hoping the technology will do its job without this attention is a dangerous position to be in," Maynard warns.

"A threat-led approach to architecting your technology stack and the people and process involved in running that technology is what is important. We take a people-first approach.

"Without the expertise to leverage the technology and configure it in a way that is optimal for the threats faced by a specific organisation, you cannot realise the full value of the technology." After all, Maynard adds, "a Formula One car is only as good as the driver behind the wheel".

For more information please visit adarma.com

ADARMA
TOGETHER WE'VE GOT THIS

Commercial feature

Why we're at a tipping point for cybersecurity

The unprecedented pace at which new threats are emerging requires a dynamic and proactive approach

Keeping on top of all the rapidly developing cybersecurity risks out there has always been a full-time job for chief information security officers and the broader C-suite. But worldwide, a cyber attack now occurs once every 39 seconds – and those being hit come from a broader range of fields than ever before.

Part of the problem is that recent technological developments and a general increase in hostility across the entire cyber landscape have combined to amplify the risks. "It's not just one thing," says Pavol Holeczy, EMEA president at ESET, a leading global digital security provider. "You don't know from where or when you'll be attacked, and attacks are becoming more complex too."

With 46% of SMEs reporting that they experienced at least one attack over the past year, according to ESET data, businesses have to keep their wits about them more than ever before. And that requires a step change in how we approach cybersecurity. ESET's latest threat report revealed a 20% increase in incidents last year. That means it's critical to keep track of the changes in the cybersecurity space and to proactively monitor your business's security.

For instance, it's no longer enough to set up a security plan and then leave it to try and handle all the various threats your organisation will face. Instead, your defences need to be proactive, probing your vulnerabilities and working to fix them before bad actors find them.

Being proactive rather than reactive is a core tenet of what ESET does. Its key principle – "progress, protected" – sums up the shift that businesses will need to undergo in order to stay ahead of hackers and cybercriminals. Indeed, some experts predict that more technological change is coming over the next 10 years than has occurred over the past century, meaning that organisations will really need to stay ahead of the curve. That means being dynamic and responding to the massive changes going on in the world of cybersecurity.

> **The more you can protect yourself, the better, especially right now, as things are changing so much**

Take the recent advancements in AI, for example. Tools such as ChatGPT can now automate the writing of phishing messages, which can be used to launch ransomware attacks against your business. In the UK alone, attacks of this kind have increased by 72% over the past year.

With the average cost of a cyber attack on a UK business standing at £3,230, any mistake can be costly for your business. And it's not just AI at play. The rise of malware as a service, the automation of various attack processes, and all the many potential future use cases for tech like AI means that cybersecurity needs to be at the forefront of your mind, rather than the last item on your meeting agendas.

That's true of big business and SMEs alike. Leveraging external expertise from the likes of ESET, which monitors and tracks changes in the cybersecurity landscape every minute of every day, can be the difference between falling foul of an attack and staying safe. ESET has 13 research centres around the world monitoring developments in the field, acting as an early warning system which can see the first signs of any new attack vectors. For instance, ESET's expert threat intelligence team has monitored the cybercrime space in Ukraine closely, warning the authorities of various potential threats.

But it's not just at a global level that ESET operates. Thousands of businesses and organisations worldwide rely on ESET to keep them safe. "Once we find a new threat, we protect everyone against it," says Holeczy. "We are constantly adding services to our products."

ESET Protect, the company's SME- and enterprise-centric platform, provides customisable security solutions, which can be managed easily either from the cloud or from your premises.

"The more you can protect yourself, the better," says Hoelczy. "Especially right now, as things are changing so much."

For more insights and advice, visit welivesecurity.com

eset
Digital Security
Progress. Protected.

Commercial feature

Science-based biometrics are the new frontier of digital trust

Generative AI has handed cyber criminals an enormous counterfeiting advantage. New solutions are required

Counterfeiting is possibly the second-oldest profession. From the ancient coin-shavers who would whittle down the precious metals to smelt them into new ones, to the dropsy-afflicted monetier Maestro Adamo, as depicted in Dante's Divine Comedy, criminals have historically gone to great lengths to deceive their victims into believing that something has more value than its actual worth.

Once, forgery required master craftspeople to ape intricate originals. It could reasonably be assumed that the more complex the object, the safer from counterfeiting it was. This logic remains with us today: the rise of biometrics – and complicated identifiers like our faces, with their many unique crypts and furrows – has deceived us into thinking that just because they are complicated, they are secure.

"Two years ago, the principal way people tried to copy and forge people's faces was using photographs or masks," says Andrew Bud, founder and CEO of iProov. These methods are, in fact, still effective in unlocking many mobile phones. However, AI technology has quickly evolved, turning these one-by-one tactics into far more sophisticated deepfake methodologies that can be deployed at scale and which are often imperceptible to the human eye. Not only are deepfakes incredibly effective, but with crime-as-a-service marketplaces doing booming business, this technology is now available for a relatively inexpensive price.

This accessibility massively expands the ecosystem of criminals with access to deepfake technology, from a select few with advanced skills and resources to criminals of even modest abilities. "It is not an exaggeration", says Bud, "to note that today's cybercriminals have mastered the art of 3D modelling to create accurate virtual representations of people, and even their ambient environments."

In 2022 alone, 'novel face swap' attacks, which superimpose identities over video streams in real time, almost trebled between the first and second halves of that year, growing by 295%. iProov, which continually monitors authentication spoof attacks via its Security Operations Center (iSOC), has noted a sizeable boost in these 'synthetic imagery injection' attacks, where forgeries are inserted into the digital pipeline to trick authenticators.

> **Accessibility massively expands the ecosystem of criminals with access to deepfake technology, from a select few with advanced skills and resources to criminals of even modest abilities**

It is not difficult to imagine how this technology could be used for nefarious purposes. From tax fraud and spoofs that fool the Know Your Customer (KYC) processes of financial institutions, to misrepresentation during remote hiring practices, these fakers aren't interested in petty crime. Instead, they're laundering significant quantities of money or getting access to sensitive data and systems to fuel terrorist activities.

Biometrics can play a critical role in helping defeat generative AI technology, and the key is liveness. "'Liveness' isn't some minor hygiene feature of biometrics on the edge of digital identity," explains Bud. "It's the central safeguard to people's digital identity. It needs to be a service, not just a piece of software that you install and forget about."

This 'liveness' is something Bud calls 'genuine presence assurance', and he believes it's the only way to get in front of these increasingly sophisticated digital injection attacks. Genuine presence assurance enables organisations to confirm that an online user is the right person, a real person and that they are authenticating in real time.

That is a complex problem to solve. One answer, though, combines science and technology by using the ambient environment to the authenticator's advantage. By sparking a series of 'illuminations' from the device camera or screen at random intervals, differences in light and shadows, almost imperceptible to the human eye, can be tested for their authenticity and compared to fakes, ensuring the person on the receiving end is three-dimensional. This one-time biometric is non-repeatable during an individual's lifetime.

As part of these protective technologies, organisations will have to build authentication platforms that are as inclusive as possible. If these measures don't include every single strata of society and work to eliminate racial, gender, age, socio-economic and other biases, they will prove woefully inadequate.

"In order to defend society and people's digital identities you have to build systems that minimise those biases," says Bud. "Inclusion is really important: you've got to be able to keep everybody safe."

For more information please visit iproov.com

iproov


Saj Dalfuge via Unsplash

COMMUNICATION

Case for the defence

As the task of managing cyber risks demands ever more expenditure, there's a growing onus on IT chiefs to keep business leaders aware of what they're getting for their money

Christine Horton

The constant battle to keep cybercriminals at bay has become a board-level concern in recent years, with defence expenditure trending ever upwards. In a tough trading period for most companies, cybersecurity budgets have largely been spared the axe, but business leaders won't keep throwing money at the task without a clear idea of the return on this considerable investment.

It's therefore down to data security chiefs to explain the risks clearly and make the case for continued investment clear to their senior colleagues, most of whom won't have in-depth knowledge of the subject.

This is even more of a communication challenge for CISOs when their audiences of board and C-suite stakeholders are focused on the bottom line. Cybersecurity doesn't generate revenue; it mitigates the risk of incurring unbudgeted costs, much like an insurance policy.

It's harder to demonstrate the value of something that averts a negative outcome than that of something that produces positive results, notes Gerard McGovern, director of digital strategy at the Tony Blair Institute for Global Change.

"Proving ROI is a challenge, because that is more the cost of not doing something," he says. "The cost for prevention is nearly always far less than the outlay required in the aftermath of any attack."

McGovern would advise CISOs to remove technical details from their explanations and make the subject as relatable as possible by reframing it.

"No one questions the need for locks and alarm systems when it comes to buildings – and it should be no different with cybersecurity," he says. "It's easy to point at all the breaches that have cost their victims millions, but that can still often be too abstract. It's better to personalise it to your organisation and explain what the potential impact would be on each of its teams."

Data security chiefs should therefore present their case in compelling terms that their leaders can relate most to. But this is easier said than done, according to Mark Wantling, CIO at the University of Salford. He believes that IT professionals typically aren't adept at speaking the language of business. As a result, cybersecurity is "still considered unapproachably technical and something of a dark art by many".

But Wantling adds that there are other effective ways to highlight the need for continued defence spending.

"I've taken to giving stakeholders live tours of the dark web. Eyes are really opened when the board sees C-level credentials for sale, hackers offering their services for as little as $2,000 and leak sites flaunting data lost to ransomware attacks," he says. "These methods demonstrate how easily poor cybersecurity can result in a breach and the potential ROI for attackers. It's not only the company's IT that's affected; the firm's reputation and bottom line are also at stake."

The ability to attach any cybersecurity investment to the enterprise's strategic objectives is key to creating a powerful argument, Wantling notes.

"When discussing anything with financially minded stakeholders, whose primary concerns are sales and operations, you must look at the organisation through their lens," he stresses. "I like to put a figure on the impact of a system outage. Our business is seasonal. If an attack were to strike home during the university's two-day clearing period, that could mean a £30m annual loss of revenue for three years. This hard figure is what I'll take to the board."

Similarly, Amanda Finch, CEO of the Chartered Institute of Information Security, argues that cybersecurity must demonstrate its value as a strategic asset to prove itself to business leaders.

"At a minimum, this means ensuring that the right key performance indicators are applied," she says. "So, instead of being measured against stats such as the number of breaches prevented, which could largely be down to luck (and in an ideal situation will be zero because of proper risk management), security should be measured against factors such as how many strategic partnerships it has enabled and business transformation projects it has supported."

Asam Malik is a partner at French auditing giant Mazars who leads its technology and digital practice in the UK. He too advocates linking cybersecurity investments to business outcomes. A bonus of this approach is that it's unlikely to cause any C-suite or board members any embarrassment over their lack of tech knowledge.

> **No one questions the need for locks and alarm systems when it comes to buildings – and it should be no different with cybersecurity**

Malik says that, when he has written a cybersecurity investment plan, he has "mapped it on to a business strategy that states 'our strategy is to grow, maintain our customers, derive more profit from our existing customer base' and so on. You explain how your cybersecurity plan will help the business achieve those objectives."

When expressed this way, it's less likely to be viewed as "a chunk of money just spent on tech", he adds.

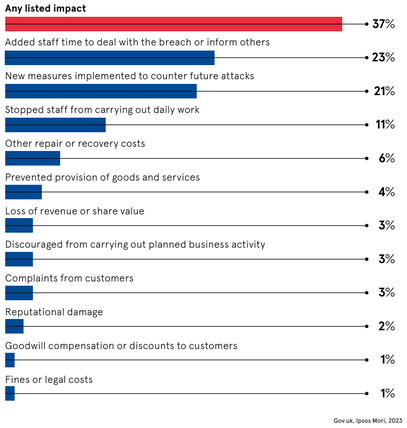
If communicated correctly, an organisation's stance on cybersecurity can even be turned into a selling point, Malik suggests.

"It's obvious to say things such as: 'If we don't do this, we could let an attack through and earn a bad reputation, causing our business to suffer.' That is true, but what we don't often mention is the other side of it: if an organisation does cybersecurity really well, it can turn this into a unique selling proposition," he says. "If we're one of those firms that holds all the accreditations and does scenario planning and regular testing, that could be a USP, as many organisations will pay more for that comfort. If execs have two or three suppliers to choose from and there's a little nervousness concerning cybersecurity, say, they'll pick the one in which they feel most confident."

The one big lesson for CISOs to take from all this is: don't make the conversation about technology risk, because an audience of business leaders will lose interest and you will lose them. Talking about the bigger strategic implications will guarantee a more successful engagement with those who will decide how much – or how little – is going to be spent on cybersecurity. ●

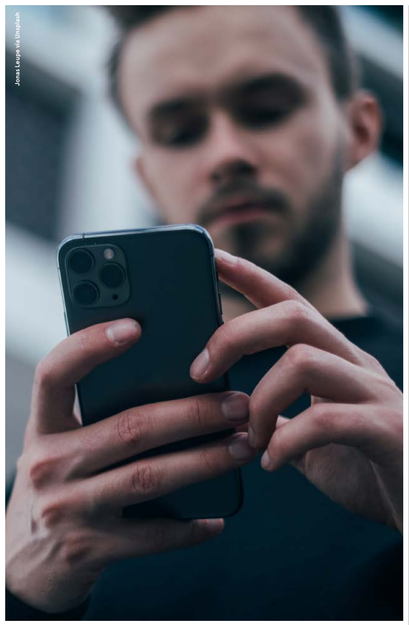
CYBER INCIDENTS ARE AFFECTING BUSINESSES IN A WIDE RANGE OF WAYS

Share of UK companies citing the following as impacts of data breaches they have suffered



Gov.uk, Ipsos Mori, 2023

Commercial feature


Jonas Leupe via Unsplash

> **Many vendor-based research reports are helpful and give good context. But the rest are just sales dressing masked as fact**

MARKETING

The profits of doom: why it's time to stop selling fear

Some cybersecurity providers use unsubstantiated research claims in their marketing campaigns to literally scare up custom. Would the sector benefit from a regulatory clampdown on this practice?

Jon Axworthy

The global cybersecurity sector will grow by more than 12% this year, according to forecasts by the International Data Corporation, so it's little wonder that the market is getting crowded with new players seeking some of the £172bn it's set to turn over in 2023.

In the UK alone, nearly 2,000 companies are offering cybersecurity products and services. That's one of the findings of a sectoral analysis published by the Department for Science, Innovation and Technology in April, which also reveals that 55% of that total are micro-businesses (those with fewer than 10 employees).

This market is a hotbed of startups, all desperate to distinguish their offerings from the competition and show potential clients that they can keep their systems safe from harm. But are some of these companies exaggerating the threats in their effort to grab attention and win business?

Playing on people's fears and uncertainties is indeed a well-known marketing ploy in the cybersecurity sector. It has been associated more with smaller entrants seeking a foothold in the market than with the established big players.

Buck Rogers is a cybersecurity expert who has worked in senior roles at the Bank of England, HSBC and BAE Systems. He is now director of the Rohkeus Cyber consultancy and professor of cybersecurity and digital innovation at the University of Gloucestershire. Rogers believes that "many vendor-based research reports are helpful and give good context, particularly the annual ones produced in partnership with various public bodies. But the rest are just sales dressing masked as fact. They confuse the picture, making it harder for people to work out how to do the right thing or buy the right solution."

He adds: "There can be a push to sell the latest thing – I get approached a lot. The greater the perception of budget or prestige, the harder the push. This practice is not helpful and it gets tiring."

Such aggressive marketing was rife in 2020-21, a time when working from home became the norm in the UK. Ransomware attacks were perceived to be on the increase and employers scrambled to shield their remote workers' systems. Information security chiefs were suddenly bombarded with buzzwords used by vendors to describe the latest vulnerability they had just uncovered and were best placed to address. They were routinely told how exposed their networks were to ransomware and urged to address the risk proactively, because such attacks were complex and costly to end.

Despite this, ransomware accounted for only 7% of attacks on British businesses over that period, according to the *Cyber Security Breaches Survey 2021* published by the Department for Digital, Culture, Media and Sport. Phishing and impersonating organisations online were actually the most common penetration methods by far.

The use of fear as a marketing tool in this sector is not new by any means. Back in 2017, Dr Ian Levy, then technical director at the UK's National Cyber Security Centre, addressed the issue at a security conference convened by *Wired*.

"The context in which you judge something also determines how you interpret it," he told delegates. "If you're told that cybersecurity attacks are perpetrated by winged ninja cyber monkeys that can compromise your machine just by thinking about it, you're going to have a fear response."

He added that vendors were "incentivised to make it sound as scary as possible because they want you to buy their magic amulets". This can persuade organisations to panic-buy inappropriate solutions, only to learn later that the threat being hyped is no more of a danger to their organisation than any other.

Roger Grimes, a cybersecurity consultant who worked as a senior security architect at Microsoft for more than a decade, notes that this can instil a "cry-wolf mentality" among the affected firms.

"It can mean that they spend too much time focusing on the wrong details and eventually become numb – until the day they miss a real threat," he explains. "I worry that we'll have a massive legacy of security systems that operate in isolation, rather than as a part of a wider security strategy, and cannot adapt to changes in the threat environment."

Two decades ago, several firms in the US financial services sector were found to have commissioned studies that served purely to market their products. The research reports they were publishing were not clear about their information sources. When the practice was exposed, industry regulators cracked down on it, imposing rules that mandated clear disclosure statements on publications and marketing materials.

Could similar measures help to clean up murky marketing practices in the cybersecurity industry?

"I'm keen for the boards that I advise to move away from the cyber Whac-A-Mole approach," Rogers says: Disclosure rules would certainly help with this. You should be able to pass *The Times* test, whereby a senior member of staff can read a cyber-based headline in *The Times* and know enough to see that in context for their organisation. The same should apply to any industry-generated threat research report. Full disclosure would provide this."

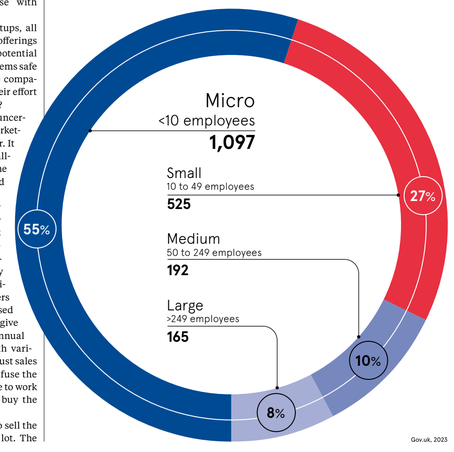
He believes that the industry could follow the lead of the medical sector, where the funding of any research, "and the impact that has had on the report's structure, are articulated clearly at the start. And, where possible, the facts and figures quoted should go through some form of independent challenge."

Without such checks and balances in place, it seems that any kind of fear-based marketing material could cloud the judgement of security chiefs and actually increase the attack surface. That's the view of Tony Pepper, co-founder and CEO of Egress, a specialist in email security. Writing an article highlighting the key findings of an Egress report entitled *Cybersecurity Hype* in October 2022, Pepper argued that his industry was "frequently guilty of selling snake oil", with outcomes often differing from expectations.

Such sharp practice erodes trust in the entire sector, which is particularly unfair on those firms that don't indulge in it. But, if the appropriate rules were enacted and enforced, startups and established players alike would have a clear set of reporting standards to work to and be held accountable for doing so. That should in turn lead to a future free from fear and doubt – in vendors' research materials, at least. ●

THE UK'S CYBERSECURITY MARKET AT A GLANCE

Registered cybersecurity businesses in the UK, categorised by size



Gov.uk, 2023

Commercial feature

Why you need to think about business continuity now

A significant deadline affecting businesses' tech stacks is approaching in 2025. That means it's time to get serious with your preparations

The cloud revolution is firmly upon us. Four in 10 organisations across Europe already use cloud computing services throughout their operations. It has, in effect, become a requirement for a modern, digital business these days to move away from on-premises and hybrid services.

"Many organisations shifted the majority of their workloads into the cloud out of necessity during the pandemic," says Richard McPhee, solutions director at Gamma, a provider of communications across Europe. "But this didn't give them the chance to consider whether their networks could handle that level of traffic when we returned to the office."

This big shift has been driven by a mix of necessity, convenience, new post-pandemic work norms and the knowledge that the cloud offers better, more reliable services than on-premises equivalents. But a looming deadline – the great copper shut-off, which is due in the UK in 2025 – is also accelerating the pace of cloud adoption.

By then, Openreach, which manages the telecommunications infrastructure in the UK, plans to have retired the old analogue phone network, which operates using copper cables, in favour of digital alternatives. This is about upgrading not just the phone system but the whole of the UK's telecommunications network.

> **The way entire networks are designed needs to be reconsidered to harness the full potential of cloud-powered services**

However, many companies' IT infrastructure remains wedded to those copper wires, with potentially damaging consequences for business continuity. "These old technologies are starting to be switched off," says McPhee. "The way entire networks are designed needs to be reconsidered to harness the full potential of cloud-powered services."

Two years may seem a world away, but the pace of cloud adoption isn't as quick as it should be, warns McPhee. Businesses are wary of lifting the lid on a Pandora's box, which could potentially require them to unpick their existing tech stack, built up over years or even decades. Overhauling the infrastructure underpinning your daily operations is a significant task, and one that often gets pushed to the bottom of the to-do list for executives and digital leaders.

Leaving it too late, though, could prove costly. With a significant proportion of businesses still needing to make the leap, there's the strong likelihood of bottlenecks in capacity and long waiting times from providers when it comes to making that transition to the replacement services. "Not everyone is aware of everything that's going to be switched off," says McPhee, noting that many systems are running on copper cables without their owners realising it.

"There are 10 million services that need to be transitioned," he adds. An entire audit is needed to ascertain how your business is exposed to copper cabling – and that takes time.

Meanwhile, the clock is still ticking. As the 2025 deadline approaches, demand will only increase, leaving laggards languishing at the back of the queue. "There is no safety net," says McPhee. When the network is switched off, it will be switched off.

That's a problem for businesses that rely on continuity of services in something as core to their operations as their IT systems. Any delay in transferring over from the current, copper wire-enabled systems to a new alternative could leave businesses unable to continue servicing their customers. The chaos that ensues could leave businesses vulnerable to cybersecurity threats in the period where they're relying on quick, temporary solutions to bridge the gap.

Starting to put your post-copper plan into action now is vital, says McPhee, because it means you'll be at the front of providers' queues to ensure that the transition is a smooth, painless one. Gamma specialises in keeping businesses moving forward by unifying the disparate communications platforms they use into a single solution to interact with clients. The company is trusted by the Open University, the Greater London Authority, and companies and charities such as the British Heart Foundation to keep communications safe, secure and standing even in the trickiest of times.

McPhee suggests that those organisations running short on time and capacity should not try to transform everything at once. In some places, it may be more appropriate to simply upgrade their existing technology to the latest version, instead of trying to overhaul their entire way of working. "We at Gamma can help with that," he says. "But if you leave it until the last minute, your back is going to be right up against the wall."

For more information please visit lp.gamma.co.uk/pstn

Gamma

Commercial feature

Why cyber risk is everybody's business

Maintaining cyber preparedness is key, especially at a time when there are more opportunities than ever for company defences to be compromised

The hybrid world of work we now operate in hasn't just transformed where we work, but also the way we work, the tools we use and how we communicate with colleagues. Email, Teams and Slack have replaced the telephone and the watercooler, and when you're not face-to-face, it's a lot harder to validate that the person on the other side of those messages is who they say they are."

That's the warning from Johan Dreyer, field CTO for EMEA at Mimecast and an expert on the changing nature of cyber risk. After all, the modern workforce may be cherishing the ability to work from anywhere, but neither they nor their employers may realise the potential danger they're in.

It sounds dramatic but, while it's encouraging to see the C-suite and boards sitting up and taking notice of cyber risk, attention doesn't necessarily mean action. For instance, in *Behind the Screens: The board's evolving perceptions of cyber risk*, a new report from Mimecast, a survey of 78 business leaders shows that chief information security officers (CISOs) routinely insist employees need to understand that cyber risk is business risk and should behave accordingly. The implication is that cybersecurity is everyone's responsibility, but with so many other distractions and competing priorities – at every level of the business – it can be easy to miss chances to improve the business's resilience.

"The cliché is that managing cyber risk is an everyone problem, but it must start with boards and senior leaders. They have to work with their chief security and data officers and security teams to define a positive and security-aware culture," Dreyer explains. "If it's role-modelled at the board and executive levels, the likelihood of it becoming part of the culture increases."

This even extends to people's personal lives outside work, Dreyer suggests. With password security and compromised credentials being one of the biggest areas of concern, the recommendation should be for people to use password managers, to remain vigilant and to avoid recycling passwords across their personal services and applications. If that can become an ingrained behaviour, the likelihood of it also bleeding into the business environment is higher.

> **The cliché is that managing cyber risk is 'an everyone problem' but it must start with boards and senior leaders**

Vigilance costs nothing

Given the complexity of cyber risk, the sophistication of attacks and the seemingly endless range of technological steps companies can take to mitigate it, some of the options for promoting cyber hygiene are surprisingly simple.

"Any part of our communications can be eavesdropped. You have to be conscious of what network you are connecting to. For instance, do you use a virtual private network, and are you really following best practice?" Dreyer asks. "When you're in a coffee shop, doing a bit of work there for a change of scenery, are you on a public network? Can you validate who is sitting around you? Laptops now have extremely high-resolution screens that can be seen from just about any angle. Just as you wouldn't discuss your bank details and passwords loudly down the phone on a train, you have to get your staff to apply similar precautions when approaching business communications."

Dreyer advocates for education and training, insisting that it must not be a punitive measure. Rather it's about encouraging and promoting good cyber hygiene. This is more important than ever given the findings of another Mimecast report, the *State of Email Security 2023*, which found that 82% of UK organisations feel they need to spend more on cybersecurity. However, businesses also routinely find they need to do more with less, and with IT spend being heavily scrutinised, security leaders are trying to reduce cost and complexity.

"The best defence will always be a layered defence," says Dreyer. "Tools should be grounded in a sense of what the organisation's risk appetite looks like. Every organisation has a different culture and view on the risks it is exposed to. So the place to start is to quantify your level of risk tolerance."

This falls under the FAIR framework – the Factor Analysis of Information Risk – which is a practical framework for understanding, measuring and analysing information risk and understanding potential loss exposure. While it doesn't make sense to apply lots of systems to something many would consider to be relatively low-risk, it's important that organisations don't just rely on the bare minimum.

For example, 94% of UK organisations think they need stronger protections than the ones that come as standard with Microsoft 365 and Google Workspace. While they are the most popular productivity tools in the business world, they are not immune to cyber attacks. In fact, their widespread adoption makes them greater targets for cybercriminals.

Hybrid cyber preparedness

So, what does this layered approach look like? To reduce business risk, organisations need to protect the work surface by layering it with a security platform that integrates with best-of-breed security solutions, and effective employee awareness training.

"Awareness training is key. It has to be understandable, relatable and meaningful," insists Dreyer. "As business leaders, we must also have processes that make it easy for employees to communicate with us – and be acknowledged for it. Consider the following for your own organisation: if you see something that isn't right, how do you make your concerns known? What support is available to help colleagues put it right?"

Rarely is a cybersecurity journey one that can be taken alone. While every organisation has an "obligation", according to Dreyer, to make progress in cyber preparedness, they also must have a clear understanding of their own limits, knowing when and how to engage specialists to help. At a time of squeezed budgets, it may seem like an outlay companies can ill afford, but "specialist advisers will be more productive and deliver quicker results", Dreyer explains.

It must also be noted that regulations and other pressures are increasing, as part of an effort to make sure companies have adequate protection in place. Without a suitable cyber policy, many businesses will find themselves uninsurable, as no one wants to take on a guaranteed risk. "Cyber insurance is applying a lot of pressure," Dreyer admits. "Requirements, premiums and co-payments are increasing due to the perceived level of risk."

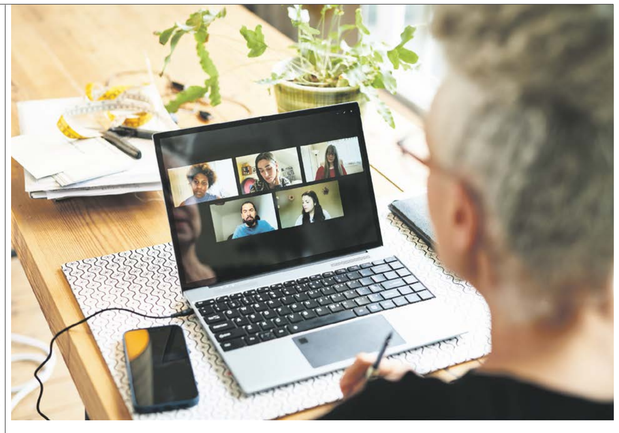
Reputationally, there is also an incentive to manage your cyber exposures. Boards are all too aware that it takes time and effort to build trust in a brand, but just moments to destroy it. They need to feel confident that the measures their security teams are taking are defensible and that they've done all they can to prevent an attack.

It is an age-old problem. All organisations are tightening their belts, and it makes sense to do so. Equally, of course, there has never been a time when a security team will say they have plenty of budget to do what they need to do.

Dreyer advises taking a practical approach to finding the best, most cost-effective solution for your own specific scenario. Consider consolidating around a smaller selection of vendors who work well together, rather than relying on a single large, consolidated vendor or many disparate solutions.

"Basic hygiene is the all-important foundation: things like password management, regular timely patching, and good configuration management. Then there are plenty of tools out there that each solve a specific threat or problem. It's easy to go overboard, but it's no use if you don't have enough people in the business with the appropriate expertise to monitor and manage them effectively," Dreyer says.

"Regularly review the configuration of your tools as compared to best practices and then identify where you might need to supplement security. Look to vendor collaborations or alliance programmes where they work together to create a multiplier effect based on the tools you already have in place today or are planning to invest in. Consider interoperability where, for (relatively) little money, you can benefit from a disproportionately large gain in security," he concludes.



8in10

UK organisations believe their company is at risk due to inadvertent data leaks caused by human error

Mimecast, 2023

For more information please visit mimecast.com

mimecast

How businesses can fight the democratisation of fraud

AI and automation have lowered the barrier to entry for online fraud. Thankfully, machine learning can help businesses improve their fraud detection and prevention

The rapid advances in artificial intelligence and automation this year are transforming the fraud landscape, making it easier for cyber criminals to commit fraud and harder for consumers and businesses to spot when they are being conned. For instance, nearly half of consumers in the US (49%) report that it has become harder to identify scams in the past six months. And businesses are seeing the downstream effects: the rate of blocked account takeover attempts – where fraudsters seek to log in to consumers' accounts using stolen credentials – jumped 427% in the first quarter of this year compared with the whole of 2022, according to data from fraud prevention specialist Sift.

> **Merchants are thankfully able to leverage technology like machine learning and be a part of global networks to prevent fraud**

"Fraudsters are using these AI tools to make their lives easier," says Brittany Allen, trust and safety architect at Sift. "They're using AI to generate more convincing written text or potentially a script that they may either read out loud or have an AI-generated voice read, and it's making it easier for them to trick victims at scale, because they come across as more convincing, more trustworthy or less identifiable as a scam."

Generative AI and automation tools are also lowering the barrier to entry for would-be fraudsters. In the past, cyber criminals often needed a high level of technical skill to commit fraud online. But now, thanks to AI and automation, cyber criminals are starting to offer fraud-as-a-service, enabling people with no technical skills to commit online fraud.

"Fraudsters who might previously have only committed fraud on their own to make money have realised that if they offer a service or if they make a tool available or assist these novice fraudsters who aren't as skilled, then they can make even more money," says Allen.

Some fraudsters are advertising so-called one-time password bots on messaging apps such as Telegram and then renting access by the month, week, day or even hour. Allen says this is effectively democratising fraud at a time when more and more people are suffering financial difficulties and could be drawn to these advertisements as an easy way to make some cash.

While these social engineering scams prey on unsuspecting consumers, businesses also need to be on alert. More than half of consumers say they shouldn't be held responsible if they are hoodwinked into providing their payment details, which are then used to make a fraudulent purchase, according to a Sift survey. Roughly a quarter say the business where the fraudulent purchase took place should be liable.

"Merchants are thankfully able to leverage technology like machine learning and be a part of global networks to prevent fraud," says Allen. "So as long as they're able to adopt technology like machine learning, which allows them to scale up and adapt to the actions of the fraudsters, they will be better set to prevent that fraud – and grow their businesses."

For instance, tech like Sift's can help businesses look for patterns in their data that could indicate a fraudster is trying to gain access to someone's account, and then take measures to prevent that fraud from taking place. This machine-learning tech aggregates data from multiple businesses, creating a network of data points that makes it even easier to spot patterns of fraud. Sift also has a community platform for fighting fraud, so that businesses can interact with each other and share best practice – a departure from the past, when businesses tended to be silent on fraud risk.

"There definitely has been a shift over the past decade, both in the willingness to communicate about fraud and in acknowledging that fraud is a common threat, and also in the availability of information," says Allen.

That change in backdrop matters. Companies that adopt real-time fraud prevention technology and share information with a network can improve fraud detection accuracy by 40%, according to Sift's research. "It takes a network to fight a network," says Allen.

For more information please visit sift.com

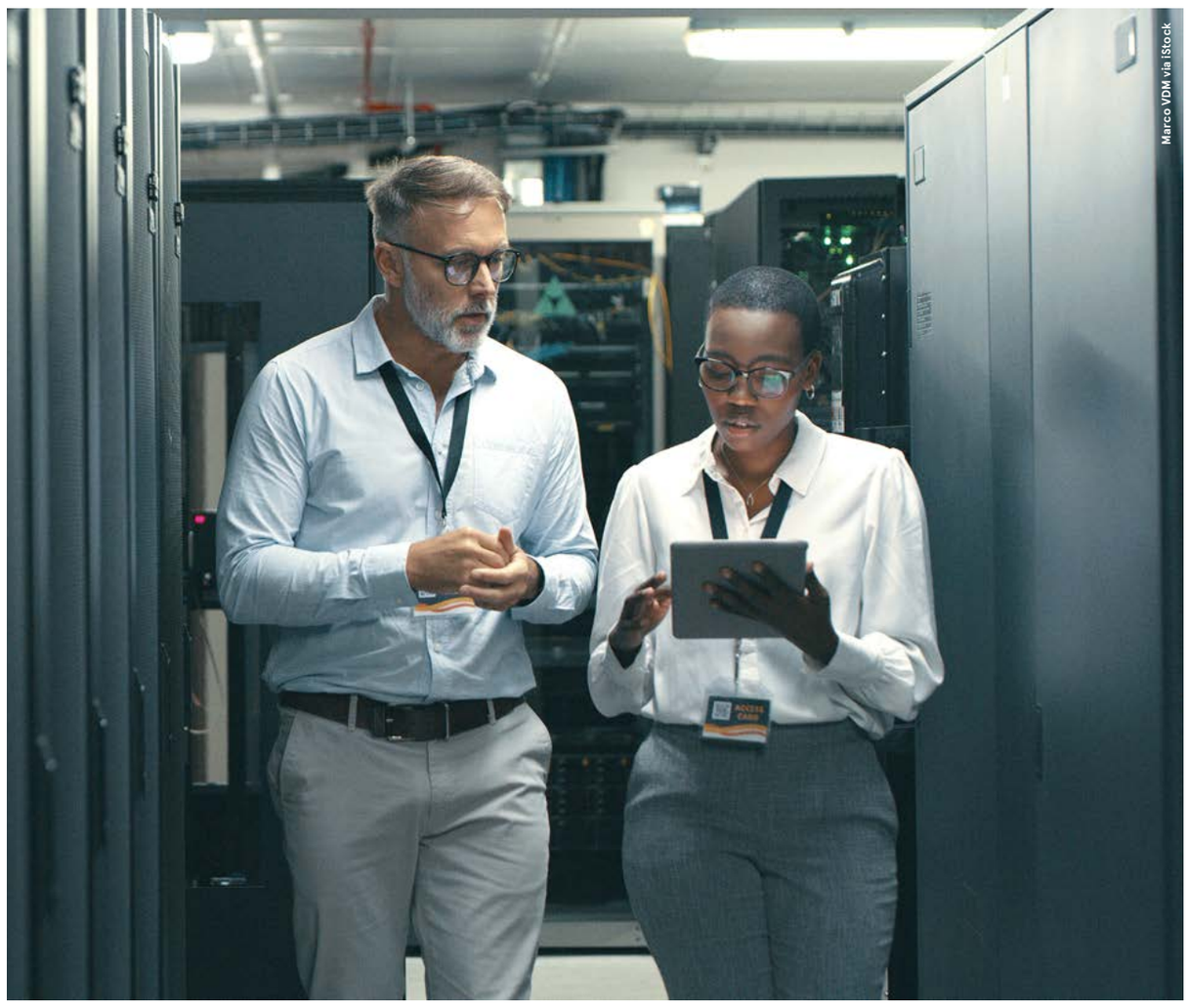
sift

PROCUREMENT

How to pick the right cybersecurity provider

The market is awash with agencies that overpromise and underdeliver. Here's the best way to identify the elite performers that will keep your IT assets safe from harm

Charles Orton-Jones


Marco VDM via iStock

Every company needs a cybersecurity partner. The question is: how do you choose the most competent one from the crowd of players offering such services? The sector has attracted a lot of newcomers in recent years and gained notoriety for spouting unsubstantiated marketing hype. This suggests that there may be plenty of wrong 'uns out there.

Philip Hoyer is EMEA field chief technology officer at Okta, a digital ID specialist based in Silicon Valley. He says that "the painful truth is that cybersecurity procurement calls for elite BS detection. Ever since the Covid digitalisation gold rush, where all firms became digital service and product companies overnight, and the shortage of experienced specialists at the enterprise level, the cybersecurity market has earned a reputation for using fear tactics to sell silver bullets."

Other common offences by providers include exaggerating their expertise and scale; aggressively marketing unproven technology; overcharging clients; and losing focus once the contract is signed.

What, then, are the hallmarks of a cybersecurity partner that can be relied upon to do none of those things?

Certification is a good indicator. A reputable provider should have all the right documents. The classics are ISO27001, Cyber Essentials Plus and Certified Information Systems Security Professional. If the firm is from the US, it should have FedRamp credentials, which indicate alignment with the government's official Federal Risk and Authorization Management Program.

Then it's time to interrogate your candidates. Claire Vandenbroecke, cybersecurity specialist at TSG, a managed IT provider, suggests the following questions to start with: "Do they have cyber insurance? Request a copy of the policy to verify exactly what is covered, such as public liability and legal expenses. Are they aware of the UK government's Network and Information Systems Regulations 2018 and how its recently announced intention to bring managed-service providers into their scope will affect their operations? Are they familiar with the Center for Internet Security's critical security controls and how these can be used to generate risk scores for organisations?"

Vandenbroecke advises checking that their claims are accurate, adding: "Request their certification number so you can verify that they're certified. And ask them to confirm the scope of their certification, because they may have had to exclude certain areas of the business to obtain it."

> **Pricing should be straightforward, providing a perspective on scalability and future costs**

With the answers to these key questions, you'll be able to make a shortlist. To winnow its constituents down to a winner, you'll need to conduct active research into the competence of each potential partner.

"Companies can request a trial period to evaluate the vendor's solutions," says Dominik Birgelen, co-founder and CEO of oneclick, a provider of cloud-hosted digital services. "This enables them to assess their usability, effectiveness and compatibility."

Birgelen suggests a proof-of-concept project to test the vendor's suitability. This should enable you to determine whether its technology integrates well with your stack.

Then there's penetration testing, which is where a white-hat hacker searches for weak points on a network. They will start by running programs to probe for flaws, often using off-the-shelf applications such as Metasploit, Wireshark and Burp Suite.

A pen tester will also, with your permission, also try social engineering. They may go phishing by emailing infected files to employees and seeing whether they download the bait, for instance. They may look for the reuse of passwords across platforms. They may call the IT team pretending to be an employee with lost credentials, bluffing their way into the system. And they may even show up at the office and try to physically gain access to systems. An unattended PC could give them the opportunity they need to inject malware into the network.

Pen testers succeed more often than not – it's usually just a matter of time and resources. Then comes the question of how far they can move within a network once they've infiltrated it. Zero-trust networks and internal perimeters should mean that access to one part of the system does not mean access to everything. Does the cybersecurity provider understand how to deploy a pen tester and respond to their findings?

There's also the matter of data location. Professor Simon Hepburn, CEO of the UK Cyber Security Council, identifies this as an important factor to take into account.

"Organisations should establish where data is held and whether the supplier's servers are hosted in the UK, the EU or overseas," he advises. "The location may affect records of processing activities and data protection officer plans under GDPR, so it's a key consideration before investing."

Naturally, a cybersecurity partner will have to do more than meet these requirements. It must be a cultural match too. This means it must listen carefully when you explain your needs. Do you want your partner to be on call 24/7 and advise the IT team comprehensively, or be less hands-on? The prevailing view in this sector is that such aspects are often overlooked.

Last but not least, there's the issue of cost. Knowing how much to pay is extremely difficult. Organisations' requirements can vary so widely that benchmarking can seem arbitrary.

"Before any decisions are made, be especially wary of overly complex pricing models." So says the founder and CEO of Arco Cyber, Matthew Helling, a man with more than 30 years' experience in this sector. He believes that quotes "should be simple and easy to understand. No business appreciates hidden costs, especially when it turns out that further funds are required after the project has been approved. Pricing should be straightforward, providing a perspective on scalability and future costs."

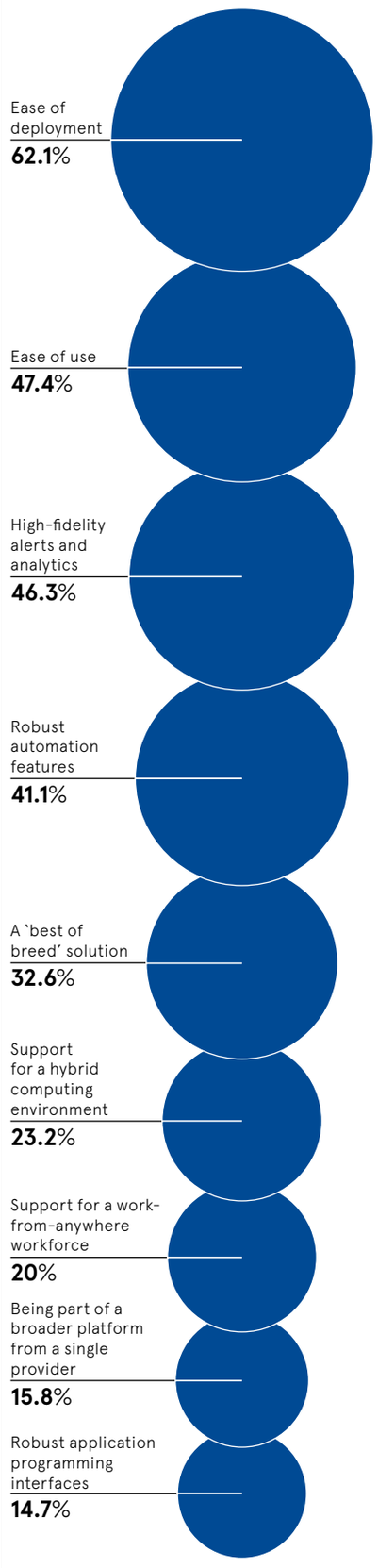
In short: if you can't understand precisely what you're paying for, something is amiss.

Is finding the right partner complex? Yes, but so is cybersecurity. Protecting your company's many IT assets – servers, PCs, tablets, mobiles and other networked hardware – from a growing arsenal of attack methods is a tough gig.

A cybersecurity partner can make the difference between the smooth running of those assets and the loss of six months' profits to a Russian ransomware gang. It's worth choosing the right one. ●

WHAT ARE SECURITY LEADERS LOOKING FOR IN A VENDOR?

Share of CISOs giving the following responses when asked which characteristics were most important in a potential cybersecurity solution



VMware, 2022

Commercial feature

How to mitigate cyber risk in a post-pandemic world

A recent survey reveals that only 28% of executives in Europe believe their organisation's cybersecurity resilience to be "very high"

When asked what keeps them up at night, the 1,300 C-suite executives globally who were interviewed, listed supply chain threats as the top risk.

Indeed, with the chain only as strong as its weakest link, supply chain ecosystems, which are often as long as they are complex, provide a weak spot that puts every global enterprise in the crosshairs of cyber criminals.

Take the BBC, British Airways, Aer Lingus and Boots for example, who this month are among a growing number of companies that have fallen victim to a third-party cyber breach. The attack, which was perpetrated by the Russian cybercriminal group, Clop, exploited a key vulnerability in MOVEit transfer software, which is used by all four organisations. From there, Clop, which specialises in ransomware and data theft attacks, was able to steal personal data including national insurance numbers and the bank details of thousands of staff.

So, why are supply chain vulnerabilities making organisations more susceptible to cyberattack? Haider Pasha, chief security officer of Palo Alto Networks for EMEA & LATAM, says, "it isn't just third-party ransomware attacks that are increasing". He notes that the overall threat landscape "continues to evolve" due to the adoption of remote and hybrid working models, plus a major shift to the cloud, which he notes "have become the new-normal in a post-pandemic world and have increased our digital attack surface significantly".

As a result, Pasha points to recent research carried out by the company's elite threat intelligence and security consulting team, Unit 42, which highlights four worrying trends.

Pasha explains: "Research by Unit 42, whose multi-layered research capability includes monitoring the dark web, has revealed that due to an increased number of enterprises embracing digital transformation over the last three years, off-the-shelf tools have lowered the barriers to entry into cybercrime. As a result, we're likely to see a new generation of cyber criminals emerge to add to the threat already posed by organised crime and state sponsored cyber groups, who frequently carry out ransomware attacks."

With a perfect storm of cyber threats having already made landfall, Pasha, who has worked in the cyber security sector for 25 years, says that organisations who want to stay one step ahead of cyber criminals "must be able to forensically analyse attacks, and the actions of perpetrators, in real time".

Pasha explains, "At Palo Alto Networks, unlike other cyber security companies, who only offer post-incident response, our unique selling point is that we join the dots and provide 80,000 customers – each of whom span the global industry value chain – with the entire life-cycle of a cyberattack."

To meet its objectives, the company, which was founded in 2005 by Israeli-American Nir Zuk, has inculcated a five-stage process within the DNA of its 13,500-plus staff.

Says Pasha, "The Prepare, Protect, Detect, Respond and Remediate methodology is at the heart of everything we do in our mission to protect endpoints, the cloud and the network of our customers."

To counter supply chain attacks, for instance, Palo Alto Network's advanced service management capabilities provides clients with a platform that tells them in real-time where their critical assets are located.

"This unique visibility not only pinpoints the location of all critical and non-critical data, but it contains another pioneering feature, which scans imported code, such as open source, for potential vulnerabilities throughout its life-cycle. This ensures that an extra layer of security is deeply embedded within the continuous integration/continuous delivery (CI/CD) pipeline."

But perhaps the greatest game-changer is that Palo Alto Networks has been using state-of-the-art artificial intelligence to power all of their leading-edge solutions for over a decade.

Pasha says, "We began using AI in our WildFires product over 10 years ago. Wildfire is a cloud-based service that provides malware sandboxing while fully integrating with the client's cloud or on-premise systems. Previously, it was the responsibility of an analyst to decide whether a suspicious file was good or bad. That job could take hours, But, with AI, we discovered that it could be completed in seconds. That was a groundbreaking moment for us as it demonstrated the power of AI to transform entire security operation centres (SOCs).

"Now we are finding that when organisations deploy the right level of good data in their SOCs, AI, which underpins our entire suite of products, can reduce the number of roles and functions in a traditional SOC team."

And the chief benefit? "It enables the same number of people to work more efficiently, effectively and towards tasks that they enjoy, such as hunting and building automation playbooks. That's a win-win for us and the organisations that we serve."

It might even mean a few extra hours of rest for sleep deprived C-suite leaders...

> **Organisations must be able to forensically analyse attacks, and the actions of perpetrators, in real time**

For more information please visit paloaltonetworks.co.uk

paloalto NETWORKS