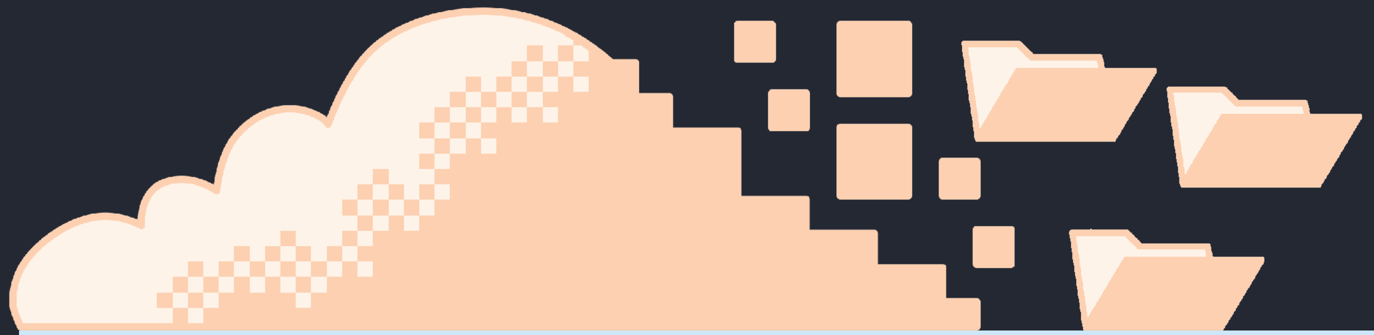
FT TECH FOR GROWTH FORUM

Technology and cyber crime: how to keep out the bad guys

The FT Tech for Growth Forum is supported by

HCLTech

Lenovo



Foreword

Visit the editorial hub at
ft.com/tech-for-growth-forum

No one today is immune to cyber crime. Even the largest and apparently best-protected companies are vulnerable to hacking, malicious data breaches, ransomware and digital extortion of all kinds. What can businesses do to respond to this technologically-enabled scourge?

This latest report from the FT's Tech for Growth Forum offers some answers – after first laying out the sheer scale of the problem.

There are cultural changes that companies can make straightaway, for instance by educating employees about the threat and ubiquity of cyber crime and by collaborating with competitors in their sector. There is also a role for government in tightening regulations.

Technology, particularly artificial intelligence, can be both an ally in the drive for greater digital security and an enemy.

Jonathan Derbyshire
Tech for Growth Forum Editor
Financial Times

Technology and cyber crime: how to keep out the bad guys

Maintaining strict security protocols and monitoring your firm's digital activity can improve your chances of fending off an attack, writes *Lucy Colback*

Cyber crime is of increasing concern to nation-states — whether the culprits are other governments or financially motivated hackers. In the US, the 2025 government budget for IT security is $13bn, up from $11.8bn the year before.

The UK, too, is wary and this extends to the risk of infiltration via allies: it has set aside £25mn to help friendly governments improve cyber security.

The private sector is also on edge. In the Systemic Risk Survey, carried out by the Bank of England and covering the second half of 2023, participants said a cyber attack was the risk that would have the greatest effect on UK financial systems. Concern was down slightly in the latest survey, published in March, but 70 per cent of respondents still put cyber crime as their number two market risk, directly below geopolitics.

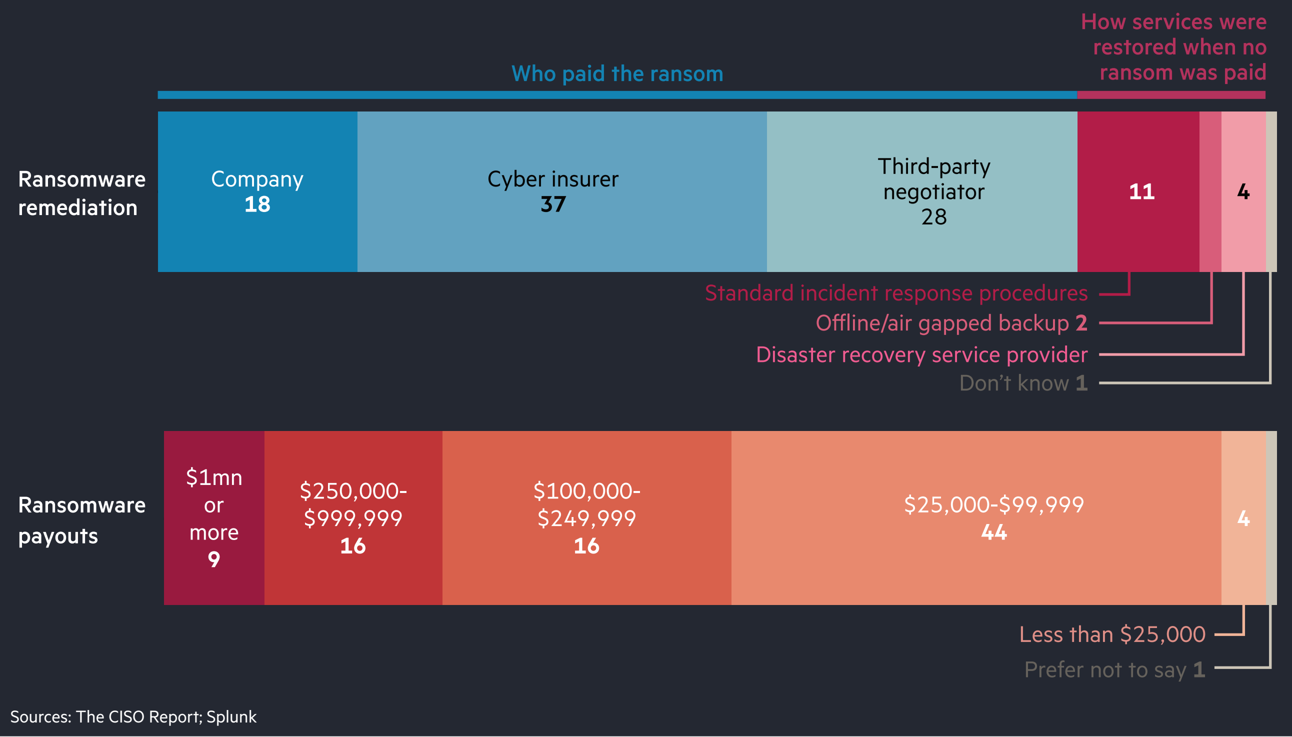
Companies are set to spend more on cyber security. A survey of 200 security professionals conducted by Infosecurity Europe found that two-thirds anticipated a budget increase in 2024 of between 10 and 100 per cent.

The threat is real, not perceived. Cyber crime is forecast to cost $9.5tn in 2024, according to Cybersecurity Ventures, up threefold on 2015.

Some 94 per cent of IT and security leaders said their business had suffered a significant cyber attack in 2023, according to a poll by Rubrik/Wakefield of 1,600 decision makers at large companies. Also 94 per cent of cloud tenants were targeted every month in 2022, a separate survey by Proofpoint, the cloud cyber security platform, said.

Ransomware: attackers get a payday

Per cent



Sources: The CISO Report; Splunk

Stick 'em up

Ransomware is a ubiquitous problem. In a traditional ransomware attack, in which files are encrypted and users' access disabled, "you have between 45 seconds and four hours before your entire network is done", says Mick Baccio, global security adviser at Splunk, a cyber security company.

One UK/US crime group, Scattered Spider, has achieved infamy for its ransomware attacks on Caesars Entertainment and MGM Resorts International.

In February 2024 Chainalysis, a blockchain data platform, said known ransomware payments in 2023 exceeded $1bn, a new high after a respite in 2022. Given the difficulty in tracking all incidents, this is probably a conservative figure. The incidence of "big game hunting" — where targets have a high value or high profile or both — has also risen. Ransoms greater than $1mn have increased as a share of the total volume of payments.

No one is immune. In the 12 months to June 2024, headline victims of ransomware included ICBC, the Chinese bank; New York state, the government body, at a key point in its budget process, and Allen & Overy, the London law firm.

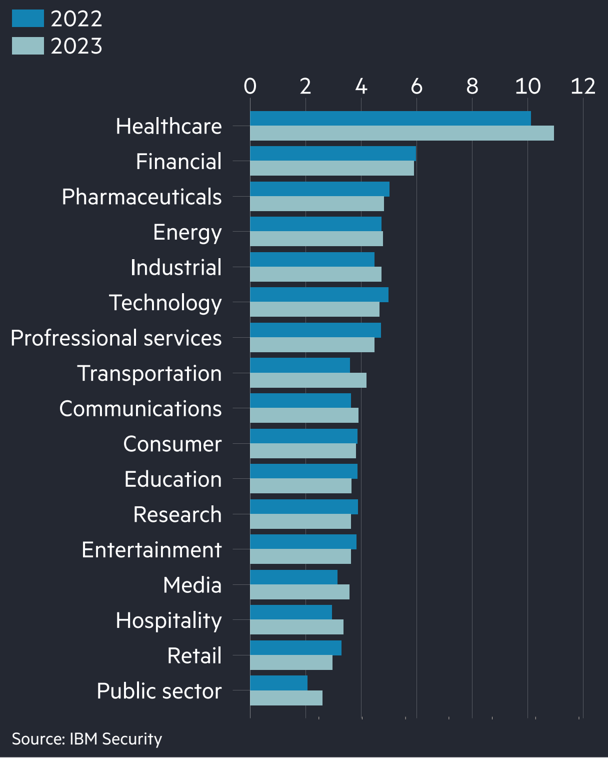
Since the start of 2023, hackers have struck at many public and private institutions. They range from hospitals, schools, government contractors and trade unions to the BBC, Royal Mail and British Airways. Of particular note was the attack on businesses across Japan after a breach at Fujitsu, the country's largest IT company.

The October 2023 attack on the British Library, only one of several knowledge repositories to be targeted in recent years, had ramifications for learning worldwide.

Cyber break-ins can cause embarrassment too: Japan's cyber security agency only found it was a victim in June 2023, several months after the initial infiltration. The 2015 hack at LastPass, the password protection company, was later linked to several crypto heists.

Cost of a data breach

By industry ($mn)



Source: IBM Security

Grabbing a byte

Data breaches can occur without ransomware. Code vulnerabilities and human error can also be to blame. IT Governance UK, a company that tracks public disclosures of data breaches and cyber attacks globally, says that by May 2024 as many records had been breached each month as in all of 2023.

Not all breaches are malicious but they can lead to data extortion. "We are hearing about this more and more," Baccio says. While security experts have become better at identifying and forestalling a ransomware attack, "any technique where all your data is gone or compromised before you know it…poses a huge, huge problem".

Given the financial motivation behind most breaches, Jeremy Hittle, chief security officer of Ridgeline, a fintech start-up, says: "One of the things I pay attention to is how someone could monetise my product in a malicious fashion." While this may be obvious for a financial services company, Hittle advises that businesses and other organisations assess the level of threat by considering how a hacker would value their data.

With or without a ransom, a breach can be costly. The experience of MGM is instructive. The company did not pay its attackers but says the incident in September 2023 cost it $100mn in earnings and a further $10mn was spent on consulting, legal and technology fees. In its 2023 annual report MGM anticipated further costs from class action lawsuits and federal investigations relating to the attack.

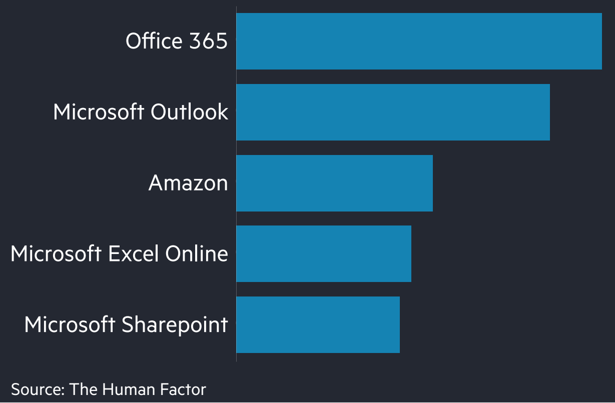
This is not to say that MGM would have been better off paying a ransom. An IBM analysis of 553 breaches (including ransomware) in 16 countries found that the average cost was $4.45mn in 2023. Companies that paid their attackers achieved only small savings over those that did not — and that excludes the cost of the ransom. What's more, 80 per cent of those that paid up were hit a second time, says Cybereason, the cyber defence platform.

While well-publicised "big game hunting" incidents have risen, small businesses are as vulnerable as ever. IBM says the average cost of a breach at a small company has grown more than for a large one.

An analysis of 1.7bn emails a day by Mimecast, the security platform, found that typical users at small- and medium-sized companies were twice as likely to encounter threats as those at large companies. Marc van Zadelhoff, CEO of Mimecast, says small companies are easier "drive-by" targets. "Hackers are constantly pinging IP addresses looking for common mistakes — and small and medium businesses just have more of them."

Top lures by software entry point

Messages



Source: The Human Factor

Social climbing

Social engineering — the art of manipulating people into giving up entry keys, passwords or other entry data — is a common way to gain access to a system. It began with the rudimentary "help me" scam emails or "reset your password" phishing mails but is now far more sophisticated. Today it can involve elaborate "pretexting", where scammers create a plausible story to lure the unwary into handing over keys.

Verizon says half of all social engineering attacks involve criminals compromising business email, which is the second most-common entry point after web applications. Such attacks doubled from 2022 to 2023. In the fourth quarter of 2023, Mimecast found that file-sharing links purporting to be from legitimate providers such as Evernote were frequently used in attempted attacks. Phishing for SME businesses' entry credentials to cloud services is common.

The cost to business is considerable. The FBI says that between 2013 and 2022, the cumulative loss from compromised email was $50bn. Of this, more than 136,000 US-based victims reported a total of $17bn losses to the FBI's Internet Crime Complaint Center (IC3).

AI is adding to the criminals' toolbox. Not only does it make phishing for email content more fluent (in English, at least), it has led to more sophisticated ploys. Sumsub, the verification software provider, points to a 700 per cent increase in deepfake incidents in the fintech sector between 2022 and 2023 and a tenfold increase across all industries. Crypto and fintech cases accounted for 96 per cent of these.

> 'The number of attacks on finance has risen'

Sector specifics

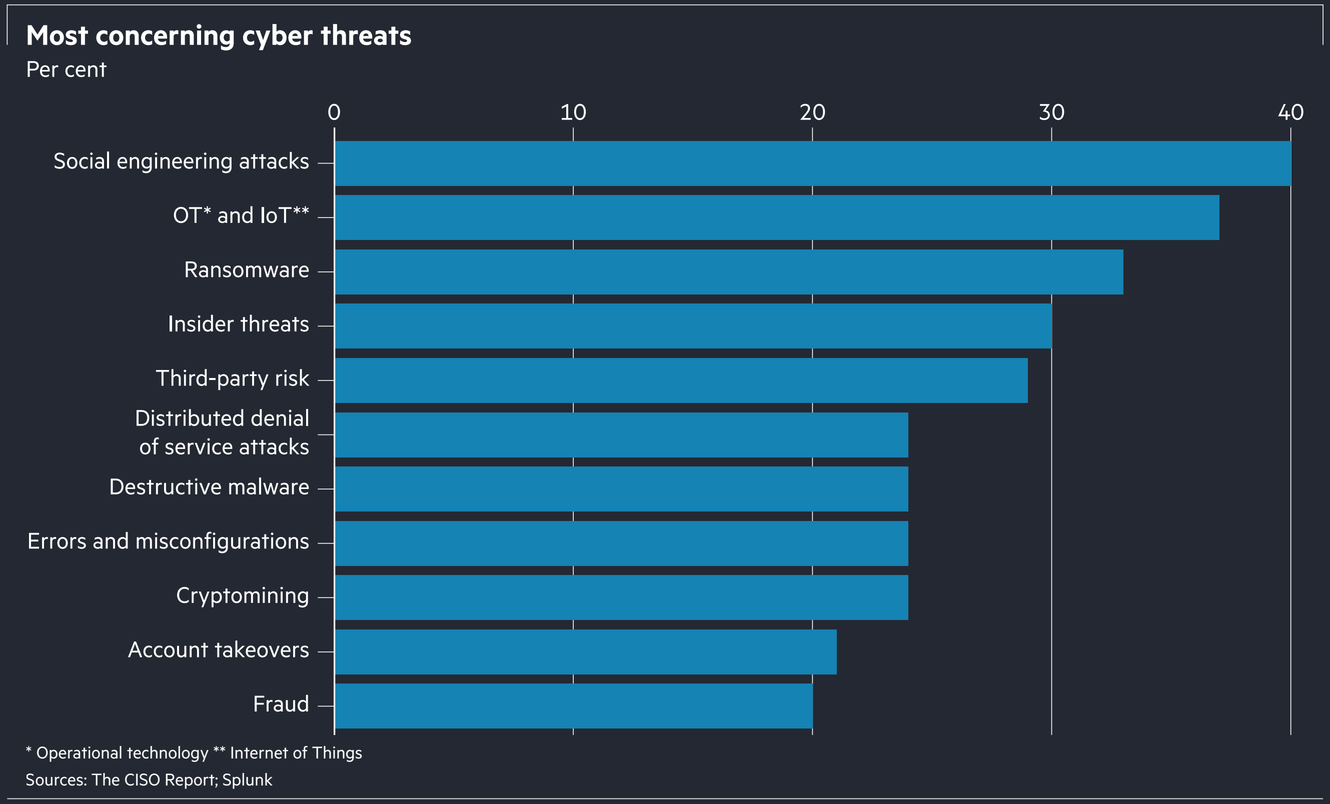
The finance sector is a prime target, for obvious reasons. Mandiant, the threat intelligence expert acquired by Google in 2022, says that 17 per cent of the intrusions it deals with hit the financial sector. Business and professional services account for 13 per cent of attacks, followed by high tech (12 per cent) and retail and hospitality (8 per cent).

The number of attacks on finance has risen. Sophos, whose report focused on financial services, noted an increase in ransomware attacks. Its 2023 State of Ransomware report, which surveyed 336 IT and security professionals in 14 countries, found that 64 per cent had been attacked in 2023, up from 55 per cent in 2022 and 34 per cent in 2021.

Some attacks have ramifications well beyond the targeted company. The November 2023 attack on the New York branch of ICBC disrupted trading in the US Treasuries market. An earlier attack on Ion Markets, the Dublin technology group, forced customers to use paper ledgers. The ICBC incident illustrated the vulnerability caused by the weakest link. Reportedly the attack succeeded because the bank had failed to patch a market system supplied by Citrix, which has 400,000 clients worldwide. The Florida company had published vulnerability updates a month earlier.

The financial sector offers crooks rich hunting grounds but every sphere has vulnerabilities. In May Mark Read, the CEO of advertising company WPP, was targeted by scammers who tried to set up a group video call. While that attempt was unsuccessful, an executive from an unnamed bank in Hong Kong was less fortunate, and this led to a loss of $25mn for UK engineering group Arup.

The cost of online payment fraud, relevant to most sectors, is also considerable. Juniper Research put the figure at $38bn in 2023, and it predicted a cumulative toll on merchants and retailers of $362bn between 2023 and 2028. There is the potential for more widespread disruption and loss. In October 2023 Lloyd's of London said a significant attack on a global payments system could cost as much as $3.5tn.



Most concerning cyber threats

Per cent

* Operational technology ** Internet of Things

Sources: The CISO Report; Splunk

Are we there yet?

More preparation is needed to even begin to match the risks. A survey of 51 countries conducted by the IMF in 2023 found that 56 per cent of central banks or supervisory authorities lacked a national cyber strategy for the finance sector. Nearly half had no cyber crime regulations and almost two-thirds did not have testing cyber security measures as a mandatory requirement.

At the industry level, the financial sector should be leading on cyber security. A KPMG survey in 2023 found that while computer crime and security was a concern for more than 71 per cent of banking CEOs, only half felt prepared. Worse, according to an EY poll, 35 per cent of directors lacked an understanding of the risks presented by AI.

Tightening regulations

New regulations mean this situation will not be tolerated. In 2022, the US introduced Circia, the Cyber Incident Reporting for Critical Infrastructure Act. America's cyber defence agency, Cisa, is now devising rules to make the country's infrastructure more secure.

Since July 2023 the Securities and Exchange Commission has required listed companies to make timely disclosure of breaches. Under older legislation, chief information security officers could be (and have been) held liable for data breaches and failing to file reports. Notable cases include that of Joe Sullivan, Uber's chief security officer, who was put on probation for covering up a data theft involving millions of his company's user records, and Timothy G Brown, the CISO of Solar Winds, who has been charged with fraud and internal control failures.

The EU is also beefing up its oversight. From October 2024 an expanded version of the Network and Information Systems Directive, NIS2, will come into force. As well as setting out fines, the directive has potential legal ramifications for managements that fail to comply with security requirements or are slow with disclosures. The number of sectors affected has grown from seven to 15 and reporting must occur within 24 hours.

Europe's financial institutions will soon be subject to the stringent requirements of the Digital Operations Resilience Act. This will take effect in January 2025 and is aimed at ensuring uninterrupted operation. Banks are likely to need to run a shadow system distinct from the one already in use, the aim being to ensure protection against cross-contamination and duplication of weakness. The secondary systems must not only run independently but be sufficiently synchronised that they can take over operations from the same point in a heartbeat. This amounts to establishing a shadow bank alongside the existing bank.

This requirement shows how much companies elsewhere need to do to address similar problems — even though the task is huge. The work involved in replicating a company's entire operational database and users' lack of familiarity with a new system are only two of the challenges.

Beyond legislation, international agencies have had some success in taking on cyber criminals. Most notably the FBI, NCA UK and Europol, working together, succeeded in February 2024 in locking out the LockBit hacking gang, which attacked Royal Mail and Boeing, from its own systems. The Counter Ransomware Initiative, whose third gathering in November 2023 was held in the US, brings together 50 countries to try to establish a common approach to combating cyber crime. Measures include enhanced information-sharing and a commitment not to pay ransoms.

How to defend yourself

Both architecture and processes must adapt to the new threat, especially in the world of hybrid access. Wendy Nather, director of strategic engagements at Cisco, says: "Most of the processes that we had when everything was on-premises were predicated on the architecture and the infrastructure, and they only worked one certain way. Now…we have to…think a lot harder about the attack surface and the different vulnerabilities and compensate for those." For instance if someone is working on two spreadsheets, one of which may be hosted in the cloud and another on their laptop, "you have to address the threat scenarios for both of those".

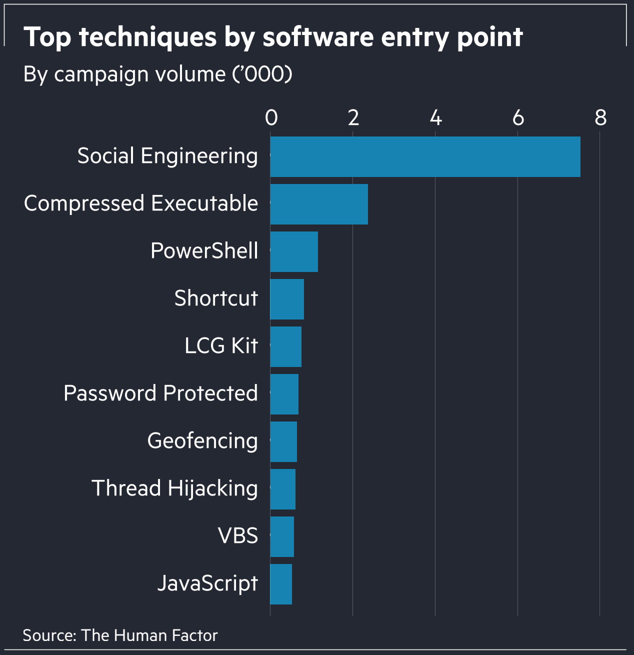
Collaborate — and report

Better collaboration — across all potential victims — is an effective way to fight cyber crime. Cooperation could still improve, a 2023 US Treasury report says. Finance companies should be sharing more information about threats, particularly when it comes to AI.

Baccio advises getting involved with ISACs — information sharing analysis centres — where industry specialists share best practice. "You may think that your security programme, your security posture, your demands are so unique and daunting. But I am positive there is someone out there that has that shared experience and can help you. Security is 100 per cent a team sport." The financial services ISAC recently established a subsidiary board in the UK.

Reporting is also key, both to promote knowledge-sharing and to bolster the chances of asset recovery. Verizon notes that collaboration between banks and law enforcement has improved the recovery rate for stolen money, while the FBI's IC3 boasts a 71 per cent success rate in recovering stolen assets.

The imperative to stay on top of developments affecting peers was demonstrated in June by the infection of over 100,000 websites which use a popular JavaScript library pollyfil.io, which enabled certain functionality in older sites. The developer warned in February that he did not own the domain name, which was purchased by a Chinese company in the same month. The attack, which misdirects website users and has as yet unknown capabilities in terms of stealing data, materialised months later.



Top techniques by software entry point

By campaign volume ('000)

Source: The Human Factor

Change the mindset

One handicap faced by security departments is that they are viewed as a cost centre. To have the best chance of repelling a threat, security has to be part of the operational fabric, from conception of strategy to execution. This extends to board representation. According to IBM, a corporate-wide security-first mindset, or DevSecOps approach (see glossary), saved companies $1.7mn compared with those who had low or no adoption.

Too much code and too many products are launched without their creators taking this approach, says Hittle, with IT security expected to make sure it is OK after the fact. "That's a losing battle, like you're always trying to secure technical debt, which is a position I never want to be in. I'd much rather consider security in the design phases."

Continued maintenance is also essential. Baccio likens this to eating your "cyber vegetables". "You know you're supposed to patch your servers, ID your assets, have multi-factor [authentication] everywhere. But you don't, and your network gets broken down. These things are related."

Web applications are the most common route to data breaches, so internet protocols such as patching servers, limiting access, using VPNs and firewalls and ensuring devices are not always connected all reduce the attack surface. Given the overlap between home and work, this mindset is important at home too.

Constant monitoring, validity checks and notifications to security personnel about unusual activity can help a company identify its own data breaches. Everything that is valuable and vulnerable must also be monitored and encrypted. This doesn't mean overseeing every cookie download, Nather says, but organisations should look out for "activity that indicates that something is going wrong — that some software or some actor is trying to take advantage of you".

"That 'something else' is what you should watch for, because that's going to happen a lot less often than accepting cookies."

This is worth it, according to IBM. The one-third of companies that identified their own breaches, rather than being told by a third party, suffered $1mn less costs on average. Involving the police or another security agency also reduced costs.

Deploy zero-trust security

Every company should run zero-trust systems so that everyone has to be verified and validated — with no exceptions. This is important given the proliferation of users in hybrid environments and the challenge of knowing who is allowed on your systems.

"For me the core [factor] is 'least privilege'," Hittle says. This means "making sure that people only have access to the things they absolutely need to have access to in order to do their jobs". Equally as important is that they only have access when they need it — and no longer. "All our access to things is 'just in time'." This request-only approach to access, which is removed when the user is done and all actions logged, means there is no "standing account lingering there, waiting to be accessed". This reduces the likelihood of an attack.

Simplify

It might seem counterintuitive but simplicity helps. Frequent changes of passwords, for instance, often means that users will apply ciphers that are easy to remember — and easy to break. Risk can be reduced by using multi-factor authentication and hardware keys that are not easily overridden by social engineering.

Hittle advocates simplicity. "When you allow a lot of things to proliferate, your attack surface can quickly grow out of control. A lens that people should put on their security is: 'What is that attack surface? How can I make it as small as possible?'"

Applying simplification can be harder for the users of legacy, on-premises technology given the bolt-on nature of their systems' development. Nather says: "Think of technology as layer cake." Any time you buy software it depends on certain layers, certain versions of software all the way down to the hardware being in a certain state. If you want to change any layer, you have to go back to the vendor of the software on top and say 'Is this OK to change?'" Certification for such a change can take months.

Go to the cloud

This is where the cloud comes in handy. Offloading more standardised functions to the cloud both simplifies the process of updates and reduces the security burden. "Things like email — there's not a lot of variation in how [it] works," Nather says. Companies can gain efficiency and boost security by identifying and relocating business functions that are similarly "well understood, not variable, well-scoped [and] that an external provider can do just as well if not better".

Baccio recommends using a guide such as Mitre's Crown Jewels Analysis to establish what should go where. "If email is my most critical asset, what are the things I need to have in place to keep email running? And when email breaks, what else breaks as a result?" Identifying the assets that you cannot function without, he says, will "determine a lot of your security posture and priority" and indicate what could go into the cloud, what stays on-premises and what needs additional security controls.

For a small company or a start-up without a huge budget, "cloud first" can be a good choice. Van Zadelhoff says. "Security skills are some of the greatest skill shortages around…cloud-based suppliers have the best security expertise and the ability to focus on that as a core competence." Larger cloud providers offer security and firewalling as standard. The off-site aspect is particularly useful for today's extended network of remote workers and various locations. The ability to apply patches to vulnerabilities and implement software updates remotely is a boon.

There are drawbacks. Hackers can exploit vulnerabilities in cloud traffic, and companies that have numerous locations — on-premises, in the cloud or both — have an increased attack surface. Infiltration can be enabled if cloud databases are open to the internet. Rubrik, the recently-listed cyber security firm, says the cloud is targeted more frequently and with more success than on-premises facilities. Almost all the cloud tenants it surveyed were targeted in 2023, with two-thirds compromised. Encryption, firewalls and segmented networks to avoid cross-contamination can mitigate some risks.

The consensus is "cloud good" but the key is to read the contract so you know where the cloud provider's responsibility ends and yours begins.

Educate

Employees frequently play a part in letting in the bad guys. Staff must be educated in hygiene and trained to spot and avoid risks. Simple actions such as not opening links on an unsolicited email can spare an organisation. The MGM hack was reportedly facilitated by the sale of weak login credentials belonging to a mid-level IT engineer.

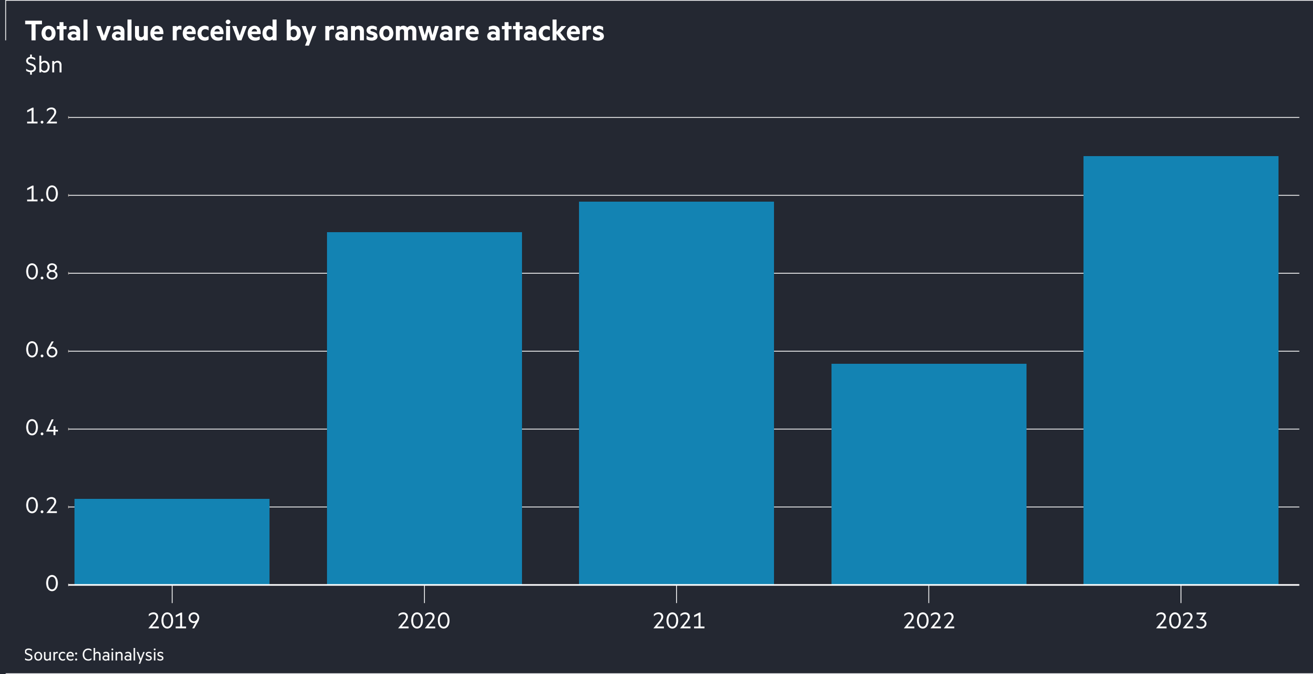
All employees should know about common pitfalls. A few bad apples, however, spoil the barrel. A study by Elevate Security, acquired by Mimecast in January 2024, revealed that 8 per cent of people were responsible for 80 per cent of mistakes that present a security threat.

To mitigate this, the company now uses AI tools that assess the content of emails in real time. When an email with a potentially malicious link or attachment is opened by someone who is high risk, a warning pops up or a 10-second video flags the threat. Education to make people wary of "channel switching with urgency" when financial topics are involved is essential. Real time interventions can save the day too. Mimecast says it blocked 250mn threats in January, the highest number experienced in its 20-year history.

Education is not only for frontline staff. Hittle says it is essential that CISOs stay up to date. "I'm a big believer in looking at as much threat intelligence as you can and processing it so you make sure it's applicable to your area of business." This way you have a better understanding of what to protect against.

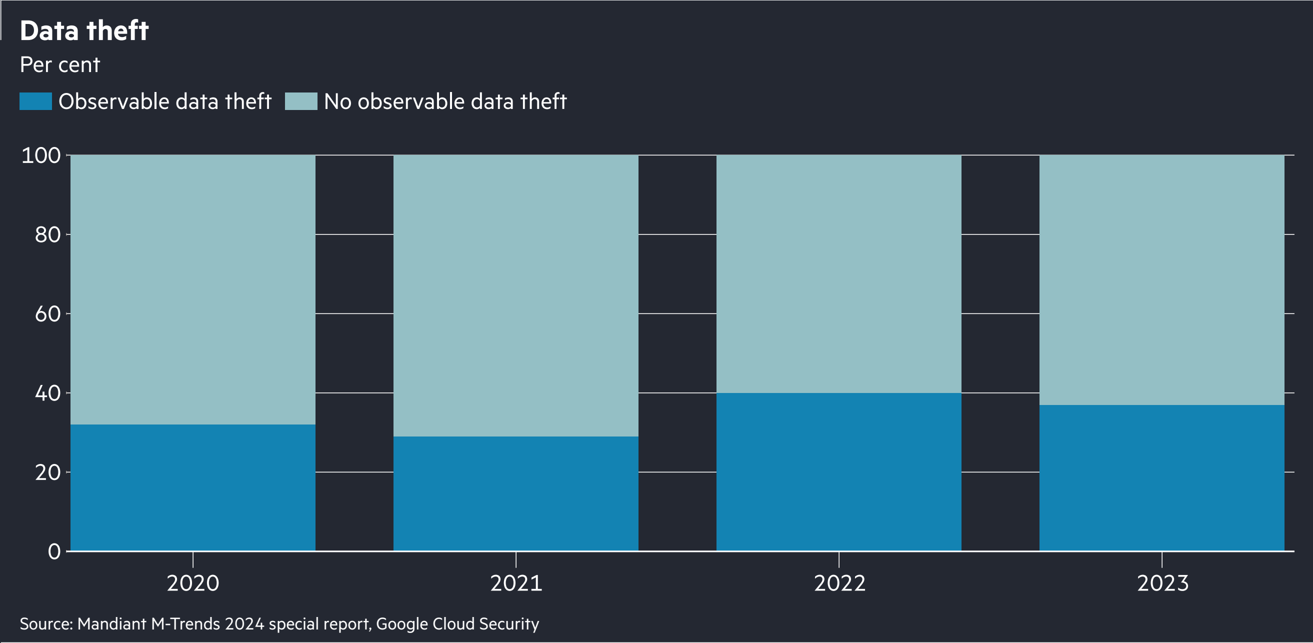
> 'The key is to know where your cloud provider's responsibility ends and yours begins'

Total value received by ransomware attackers



Source: Chainalysis

Data theft



Source: Mandiant M-Trends 2024 special report, Google Cloud Security

Enlist AI — and have a coherent policy on its use

The proliferation of AI tools means that this technology has to be considered from various angles, some of which have been addressed above. When it comes to the in-house, day-to-day use of tools such as generative AI, a coherent policy is vital. It is a risk in itself if AI is allowed to run rampant in a business that does not issue a clear direction on who can use it and how.

Despite this, guidance on AI use is rare. Splunk's State of Security report on AI says that almost all companies use AI but only two-thirds have organisation-wide policies. Baccio says: "The lack of education around [generative AI] is a big concern", notably when it comes to using a leased "slice" of a public model. One nightmare scenario would be: "Did you just throw proprietary company data inside this LLM [large language model]? Because we can't get it out."

There is also a potential for the public LLM to be "poisoned"— and your data with it. One possible solution is to have an "air-gapped" LLM that cannot connect to the public internet, such as the one now used by the US Department of Defense.

Every policy must be clear on what AI can and cannot be used for, Baccio says, but the specifics depend on the organisation and the collaboration of all stakeholders. Those involved might include a chief data officer or chief data scientist, the legal team and security team as well as potential users. The legal team or risk management might decide the final form.

When it comes to using AI for cyber security itself, the arms race between good guys and bad guys is well under way. Tools rolled out by the defence include Sumsub's deepfake detection, Mastercard's Decision Intelligence (DI Pro) — which scans data points to detect fraud — and email analysis tools such as those outlined by Mimecast, above. Generative AI can be used internally to identify gaps in security measures or to help train employees and customers in cyber security and detection.

In a webinar, Nikesh Arora, CEO of Palo Alto, said AI with natural language capabilities would help solve the shortage in cyber skills. It could make products simpler to use and so reduce the need to train more IT experts. AI might also expand real-time monitoring and accelerate response times to an attack.

Nather says AI will be able to incorporate institutional knowledge, for instance learning how an organisation uses technology along with threat intelligence. "With AI we can train the systems to understand better what looks normal or what's within the range of normal. Then we can advise the customer 'This looks strange to us…[and] this is why'." This can be done in natural language instead of some "very obscure error message" which requires expert interpretation.

After AI, the next frontier is likely to be quantum computing which will be a mixed blessing. It could help both with encryption and cracking it.

> 'Keep it simple, plan your response, find a breach quickly, report it early'

Vet your digital supply chain

It is important to perform due diligence on any supplier, and this goes for cloud providers too. Thales Cloud Security Study 2023 said more than three-quarters of respondents to its survey used more than one cloud supplier, while three-quarters said 40 per cent or more of their cloud data is sensitive. Only 2 per cent encrypted all their sensitive cloud-hosted data.

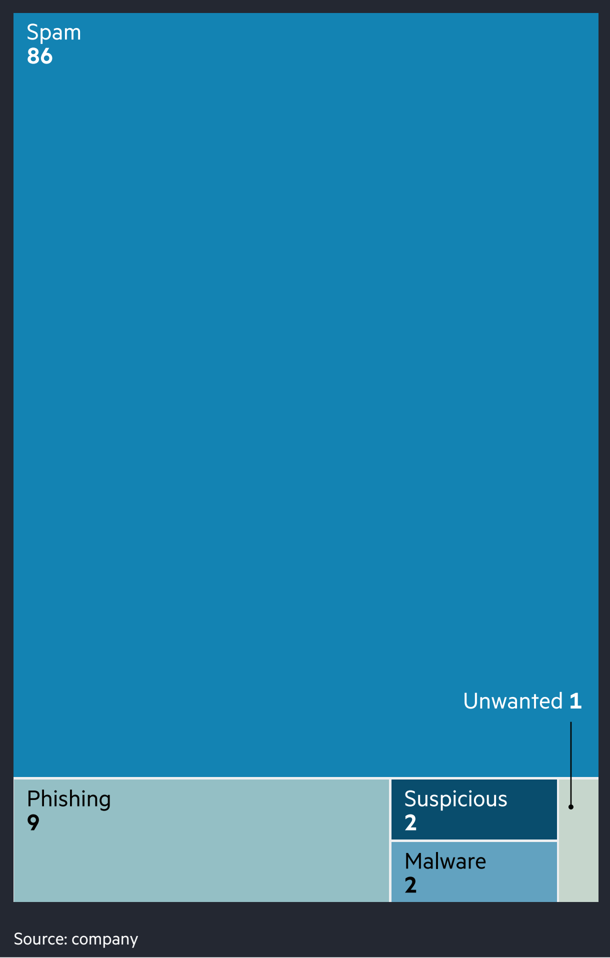
Have a robust vendor risk-management programme and regularly review the people you use — but try not to have too many. "A lot of companies [increase] their risk profile by adding more and more vendors," Hittle says. Not all sellers are created equal. It's really important to do deep security vetting of all vendors. Certifications can help with this, such as the Star cloud security alliance or ISO, but doing your own work is important, for example ensuring that the auditor who grants a certification is reliable and reputable.

Those undertaking mergers and acquisitions should regard this extra layer of security as due diligence, Baccio says. "When your organisation purchases another one through M&A, you inherit all of those assets. Are they patched? Are they accounted for? Are they identified? If they're not, you're inheriting that organisation's security posture…and the risk posture that comes with it."

Indicating the vulnerability of small companies to a supplier attack, in June the operations of around 15,000 auto dealers were affected by a hack of CDK Global, the specialist cloud software provider.

Mimecast's top threats based on email analysis

Relative volume of all threats (%)



Source: company

Have a plan

Prevention is better than cure but in the event of a breach it is critical that a company has thought ahead. Have a response plan and team in place. Have a secondary system if possible. Have all data backed up so that you can bring them online when frontline systems are compromised. Bear in mind that these are also targeted by cyber criminals, so they too must be watertight. Is your plan up to the task?

Companies need a robust strategy for data replication so that if they must switch systems, data are not compromised or corrupted.

This might be easier for cloud-first and digital-first businesses than for on-premises companies or those with legacy technology, but the latter, too, have to find a solution. Financial services companies that will be affected by the EU's Dora should be ahead on this.

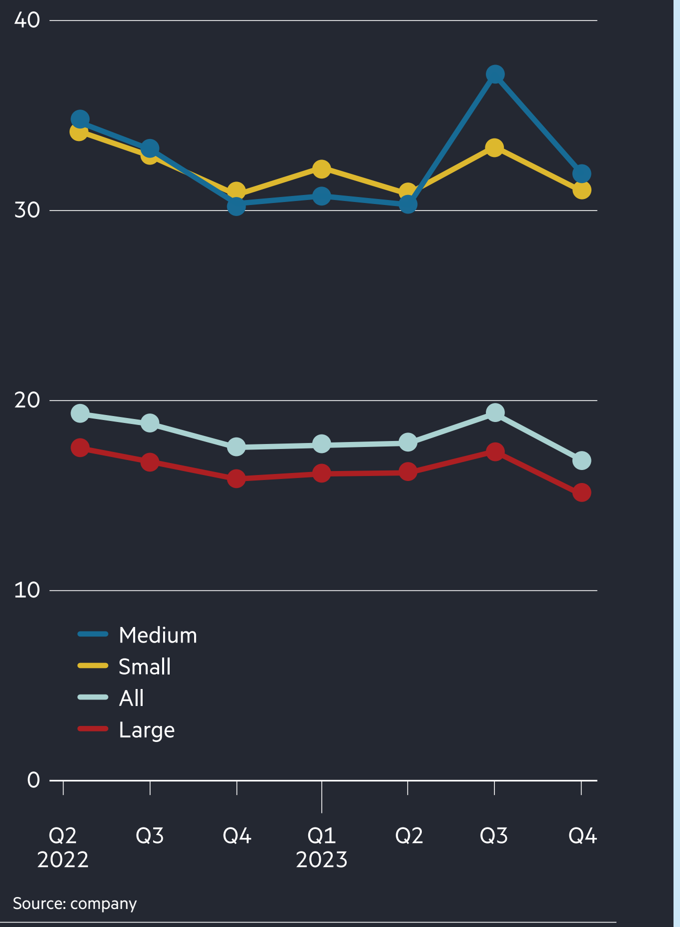
In the worst case, go back to basics. People need to know what they should do in the event of a cyber emergency, even if that means sending someone out to buy more laptops or having staff go to a local café with their personal devices to continue operations.

Cyber insurance can be the last line of defence but it can also encourage more attacks — although the National Cyber Security Centre in the UK believes the risk of being targeted due to having insurance cover is overstated.

A helpful mantra for the security mindset might be: keep it simple, plan your response, find a breach quickly, report it early.

Mimecast on vulnerabilities based on email analysis

Threats by user company size



Source: company

Glossary

- **Attack surface**
  The number of possible points for unauthorised entry into a user's system.
- **Malware**
  Malicious software run on a system that alters function without the owner's consent, for example viruses, spyware, a backdoor attack.
- **Hacking**
  Illegitimate attempts to gain access to or harm IT assets such as brute force, denial of service, injection of malicious coding into web pages.
- **Social engineering**
  Exploitation of people to gain access to assets, for instance through phishing, blackmail, scams, threats.
- **Pretexting**
  A form of social engineering that uses a story or pretext to gain a victim's trust and then manipulates them to gain access to assets.
- **Smishing**
  More social engineering, this time using fake mobile texts to gain access. Beware your unwary link-clicker ("we tried to deliver a parcel…"). Pretexting is another issue.
- **Vector**
  A means by which entry is gained, for example, web, email, backdoor, carelessness, error, malware download etc.
- **DevSecOps**
  A portmanteau of development, security operations. Essentially the team that ensures security is integrated at every stage of the development and implementation of software design.

Premium Members

The FT Tech for Growth Forum is supported by *HCLTech* and *Lenovo*, our premium members, who help to fund the reports.

Our members share their business perspective on the forum advisory board. They discuss topics that the forum should cover but the final decision rests with the editorial director. The reports are written by a Financial Times journalist and are editorially independent.

Members' views stand alone. They are separate from the FT and the FT Tech for Growth Forum.

Why your culture is your best shot against deepfakes and other advances in social engineering

Doug Fisher, senior vice-president and chief security officer, Lenovo

Cyber crime today is a seriously lucrative business. It is hardly surprising that criminal organisations are employing specialist developers and social engineering experts to deploy cutting-edge strategies that can exploit any gap in your defences.

This means it is impossible to keep an organisation 100 per cent secure. That challenge is becoming more pronounced now that hackers have turned to AI and other new technologies.

Since AI became widely available, some employees have been tricked into transferring millions of dollars into fraudsters' banks. They were taken in by deepfakes in videoconferences and believed that their managers wanted them to move the money.

Sadly this is only a taste of what is to come. If there is money to be made, hackers will continue to come up with new and sophisticated means of attack.

If you can't stop an attack, what should you do? Put simply, you should make the hackers' job as time-consuming and unprofitable as possible. If you undermine their return on investment, your business is significantly less attractive as a target.

At Lenovo, we have a security-minded culture that extends across the entire enterprise. Recognising that human error is to blame in at least 68 per cent of cyber incidents*, we make it mandatory that every employee completes a thorough cyber-awareness programme — no excuses!

If we find someone who is not compliant, or who has not added the latest security upgrades to their PC, we shut off their access until they are up to speed, no matter their seniority. Lenovo's leadership has embraced this mindset and we have achieved near-total compliance.

We extend zero-tolerance to our supply chain. Because hackers could compromise the electronic components in our devices, it is our responsibility to do everything we can to make the manufacturing process secure.

We own many of our factories so we can control physical security and who gets access. We also vet the security processes at 1,100 suppliers. We have joined with Intel and AMD to produce a supply chain platform that lets customers see all active component elements in a product. They are then able to ensure that none has been tampered with since the unit left the factory.

Although AI is being used by hackers it is also a powerful security tool. We use the technology to enhance threat detection, incident response and vulnerability management. It can also be adapted for training, to simulate threats and to find holes in existing protocols.

Cyber crime is not going away. A rigorous, consistently enforced culture is no guarantee of resilience but it is an extremely good start.

** Verizon 2024 Data Breach Investigations Report*

About the FT Tech for Growth Forum

The forum takes a unique perspective on how technology can be used to achieve the objectives of businesses and society as a whole.

Through reports, events and the sharing of expertise, we seek to help leaders in business and politics understand how technology can help with change.

Find out how to take part in the FT Tech for Growth Forum by emailing
forums@ft.com