Navigating Cyber Risk

Wednesday June 1 2022 www.ft.com/reports

Conflict increases hacking threat

Inside Energy plants in power play *Page 4* ● Smart factories get smarter *Page 7* ● Transport: a moving target *Page 8*

Inside

Energy plants at risk in cyber power play
Russian hackers are turning electricity grids and pipelines into a new theatre of war

Page 4

Banks' digital push is Pandora's Box moment
Remote working and online transactions have unleashed new threats
Page 4

Smart factories need smarter IT
Connected machinery and complex supply chains need protection
Page 7

Transport: a moving target for hackers
Cyber attacks can be aimed at critical national infrastructure as well as the valuable passenger payment data held by air and rail groups

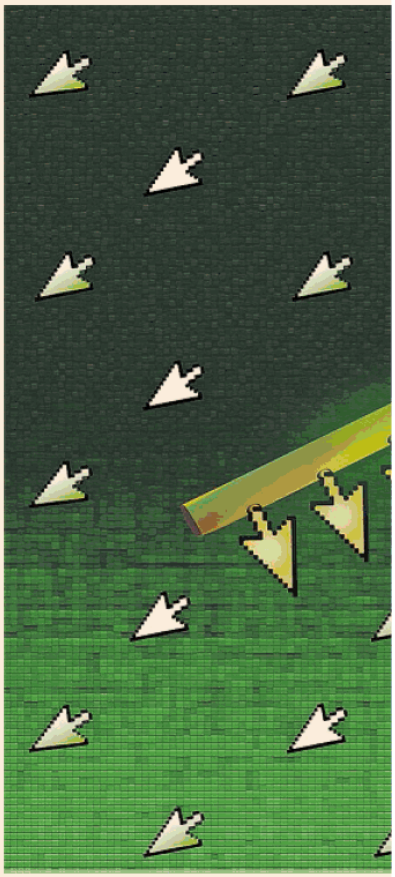
Page 8

Hotels wary of unwelcome guests
Cyber criminals try to infiltrate booking systems and WiFi
Page 10

More online

COVID AND CYBER RISK
How contact tracing posed a new data challenge for the hospitality industry
www.ft.com/cyber-risk

If you can't stop them, disrupt them



IT systems

Best defence can be spotting weaknesses and slowing attacks, says *Hannah Murphy*

For decades, companies have bolstered their cyber defences in a bid to thwart intruders. But while this work will always continue, firms are increasingly confronting the reality that it takes only a small slip-up, or an unnoticed flaw, for hackers to be able to get inside their systems. And then what?

So, in a shake-up of approach, many businesses are now focusing on how to mitigate cyber attacks — on the assumption that a breach is inevitable.

Some firms create internal "red teams" to probe their own systems for weaknesses, but Padraic O'Reilly, chief product officer and co-founder of cyber security risk group CyberSaint, says companies should do more "proactive or mitigative remediation".

"You will be planning for budget cycles, and looking at risk and making risk-informed decisions, instead of just putting out fires."

This shift comes as several highly sophisticated nation-state cyber campaigns — such as the SolarWinds hack, which even hit government agencies — have demonstrated that companies can be unknowingly vulnerable if there is just one weak link in their supply chain.

Meanwhile, ransomware attacks — in which cyber criminals encrypt an organisation's data and demand money for releasing it — have escalated. Companies in all industries have been targeted. Data from SonicWall show a 105 per cent rise in ransomware attacks in 2021.

"The ransomware problem has become so pervasive," warns Andrew Rubin, chief executive of security group Illumio. "That proved to everybody that you're going to get hit almost no matter what, which is not a failure of your cyber strategy, it just means that you have to evolve your cyber strategy to both detect, as well as stop, the spread."

One emerging field for protecting operational technology — such as critical national infrastructure, manufacturing facilities, automotive plants, and aerospace systems — is CCE or "consequence-driven, cyber-informed engineering".

According to Stuart McKenzie, senior vice-president of Mandiant Services in Europe, Middle East, and Africa, the CCE methodology first requires companies to conduct a "crown jewels assessment" of their business from an operational perspective — establishing any elements of production that need to be operationally effective 24/7.

So-called "consequence prioritisation" is vital in making sure that electricity blackouts are avoided, and water treatment can continue, for example.

McKenzie says it is about asking the question: "How do we protect these critical assets and then, once we got something around those, look at the

Industry leaders gain 'false sense of cyber security'

Company policies

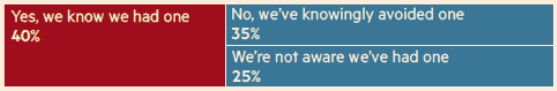
Survey of 350 US and European manufacturers shows more confidence than best practice, writes *Matthew Vincent*

Three quarters of manufacturing companies claim they are aware of cyber risks and can deal with most of them — but, in reality, many still lack the skills and security practices to do so, new research has found.

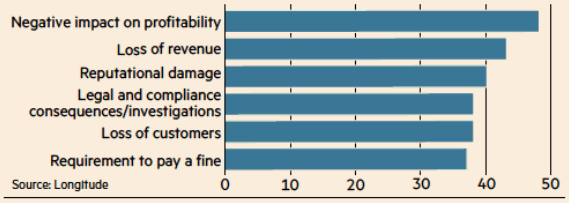
In a survey of 350 industrial groups across Europe and the US, conducted by the Financial Times' Longitude research and consulting business, 75 per cent reported that they either knew of a cyber attack being mounted against their operations (40 per cent) or had knowingly avoided an attack (35 per cent).

Among those that did suffer a cyber attack or data breach, nearly half said it dented their profits, while four in 10 acknowledged there had been reputational damage as a result, and a reduction in sales. Medium-sized companies, with a valuation between

Manufacturers are under attack from cyber criminals –and the consequences are significant
Have you suffered a cyber attack of any kind in the last 12 months?

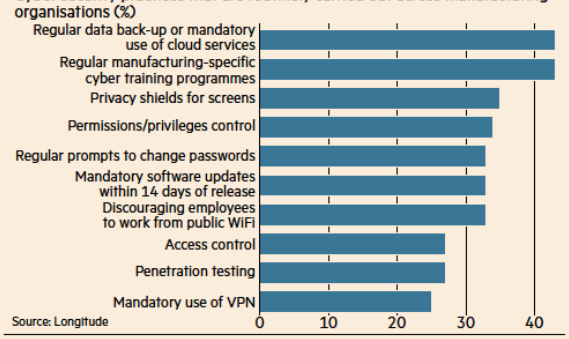


Direct consequences felt by manufacturers who have suffered a cyber attack



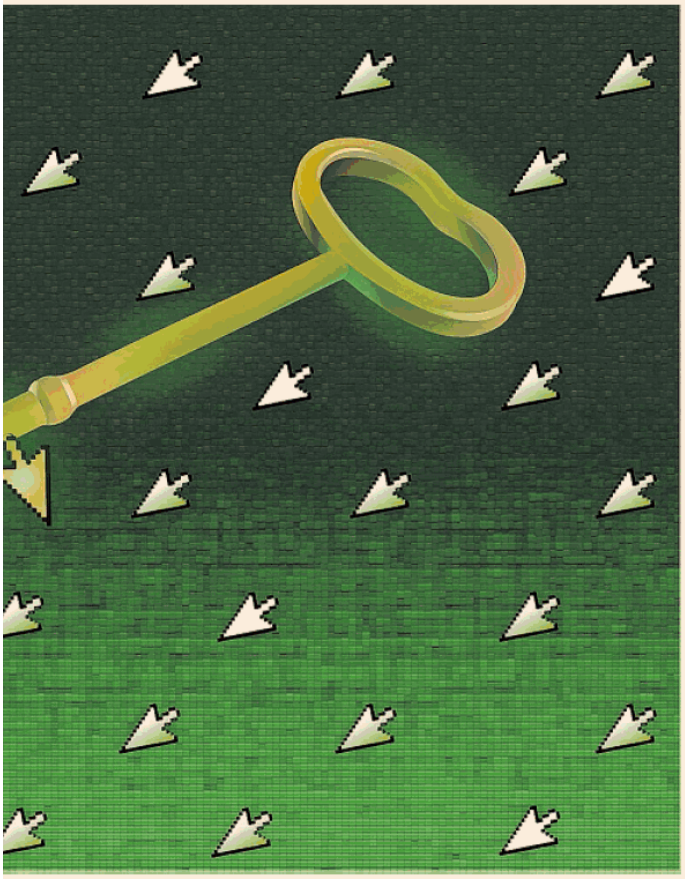
Source: Longitude

Manufacturers have poor cyber hygiene
Cyber security practices that are routinely carried out across manufacturing organisations (%)



Source: Longitude

Navigating Cyber Risk



next layer and then look at the next layer?"

Idaho National Laboratory, which developed the framework, calls for a "system-of-systems analysis" — in other words, identifying interdependencies between systems and their components.

After that, the next step is dubbed "consequence-based targeting": essentially mapping out the ways in which an attack might progress around a target's computer systems and cause the most damage. It involves working out "where they need to be to conduct the attack, and what information is required to achieve those goals", says the INL.

When this attack path mapping is done, it is down to engineers to disrupt those digital assault pathways, where they can.

Companies must assess "the threats and scenarios that an organisation faces and then play those through their systems, their processes, their business, to see where weaknesses would occur", says Del Heppenstall, cyber security partner at KPMG.

This might include more conceptual "tabletop scenario-driven exercises which step through 'what ifs'. If this happens, then what?". Or it might involve more "hands on" testing, he adds. "Some clients, ultimately, want to test the resilience of their live environments."

Mitigation measures can take multiple forms. One key approach to it is 'segmentation', or dividing a network into smaller parts, according to Illumio's Rubin.

He uses the metaphor of a submarine split into an array of compartments: if a leak springs, it will only affect one small compartment rather than flood the entire submarine. "Segmentation is getting . . . a ton more attention than it ever has," Rubin says.

Detection and having visibility over systems is also vital. This can be helped by tools that carry out "scanning for anomalies", says Heppenstall. Another element is making comprehensive incident response preparations.

"It is worthwhile to be prepared, to put into practice the ability to respond, to validate that your controls and everything is working as intended," says Joe McMann, Capgemini's global cyber security portfolio head. That way, "when you do have a problem, you know exactly what to do, you're not scrambling," he notes.

However, McCann acknowledges that, for companies, there remains the age-old problem of trying to validate the return on an investment in security.

Cyber attack mitigation becomes part of the corporate risk management process: "It is a risk-based, cost-based decision that every business and every enterprise has to go through to weigh the pros and cons of implementing a program that would prevent impact from a certain risk in their enterprise," he says.

Contributors

Hannah Murphy
Tech correspondent

Sylvia Pfeifer
Industry correspondent

Nick Huber
Freelance journalist

Alice Hancock
Leisure industries reporter

Kevin O'Rourke
Group head of risk management, Bank ABC

Peter Chapman
Matthew Vincent
Commissioning editors

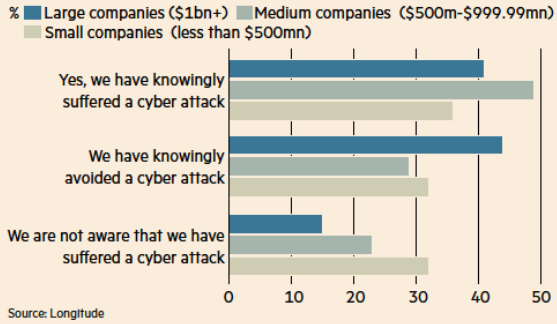
Efi Chalikopoulou
Illustrator

Steven Bird
Designer

Esan Swan
Picture editor

For advertising details, contact:
Stefan De Muynck
stefan.de.muynck@consultants.ft.com
+352 691 635 989

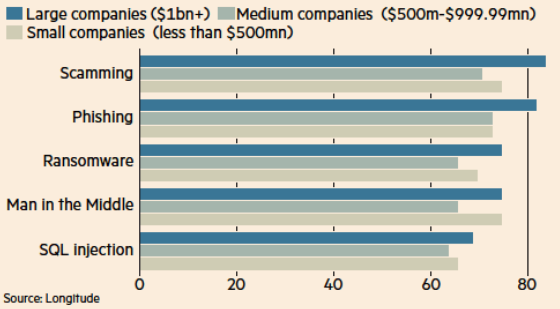
The 'squeezed middle' are more likely to suffer a cyber attack



Source: Longitude

The 'squeezed middle' are less prepared for cyber threats

Manufacturers that feel fairly or very well prepared to deal with the following cyber attacks (%)



Source: Longitude

Cyber governance is poor in manufacturers

Cyber security governance in place across manufacturing organisations (%)

Source: Longitude

$500mn and $1bn, emerged as the most likely to be successfully targeted by hackers or cyber criminals, with 49 per cent admitting they had "knowingly suffered a cyber attack". In comparison, only 41 per cent of $1bn-plus groups and 36 per cent of smaller, sub-$500mn businesses knew of attacks. Large companies were the most likely to have knowingly avoided an attack: 44 per cent said they had managed to do so, against only 29 per cent of medium-sized businesses.

But, despite their greater vulnerability, the "squeezed middle'" of the manufacturing industry appears to be less well prepared for cyber attacks than larger or smaller groups. Of the five common types of attack, medium-sized companies had the lowest level of preparedness for four of them: scamming; phishing (where fraudsters trick businesses into disclosing payment information); "man-in-the-middle" attacks (where criminals intercept and change secure messages between parties); ransomware (where data is 'locked' with encryption and only released for a ransom); and SQL injection (where a malicious code is used to access databases).

And "cyber hygiene" — the carrying out of appropriate security practices — was found to be poor across companies of all sizes. Only a quarter made connecting via virtual private networks mandatory; only a third prompted staff to change passwords and demanded mandatory software updates; fewer than half backed up data regularly or arranged industry-specific cyber training.

Senior management often failed to ensure sound systems of cyber governance were in place. Only 36 per cent of manufacturing groups gave a board member direct responsibility for cyber security, or reported on it every year. Fewer than half operated a company-wide security policy or made staff throughout their businesses accountable for cyber safety.

Longitude's survey did find that a small number of manufacturers were taking effective steps to protect their operations — by investing in technology, insurance and specialist advice. More than half are now investing more in cloud computing security measures, safeguarding their computer networks, and preventing attacks via interconnected devices (the "internet of things").

However, the disparity between most companies' stated confidence and their limited skillsets and preparations led the researchers to question their "false sense of security".

Infrastructure Russian hackers treat grids and pipes as theatre of war, says *Hannah Murphy*

Energy plants at risk in cyber power play

US oil refineries have been targeted by hackers
Gary Coronado/ Getty Images

In 2017, a Russian hacker came within a whisker of causing what could have been a "catastrophic" and deadly attack on a US oil refinery, according to a Department of Justice indictment. The hacker got into the refinery's systems and deployed malicious software with a view to causing severe "physical damage" — but, instead, triggered safety systems and automatic shutdowns of the refinery.

In March, the hacker — an employee of the Russian defence ministry's research institute — was charged by the DoJ, alongside three other Russian government employees who allegedly targeted energy companies across more than 135 countries between 2012 and 2018.

These charges reflect an increasingly strident approach by the US government in its pursuit and prosecution of cyber adversaries. However, they also reveal the ongoing appetite among nation-state hackers to target energy companies, to cause maximum disruption. While the energy sector has long been a top target for hackers, cyber security experts are now warning of heightened threats amid the Russian invasion of Ukraine, and are urging the industry to take more decisive action.

Russia is treating cyber as an "additional theatre of warfare", explains Stuart McKenzie, senior vice-president of Mandiant Services in Europe, Middle East, and Africa.

Targeting critical energy infrastructure is "how you can have the biggest impact — it's an ability to really show an extension of your power", he says. More than causing disruption, it can "really erode the public's perception about your ability to protect".

Early this year, the discovery of "wiper" malware in Ukraine, which permanently deletes data on infected computers, sent shockwaves through the energy community and raised fears it could spread across borders. Then, in April, the Ukrainian government also revealed that it had thwarted an attempt by attackers from Sandworm, a Russian cyber-military unit, to hack high-voltage electrical substations. In a research note, analysts at Moody's warned that, given the interconnected nature of European electricity grids and gas pipelines, "there is increased risk of a cyber event impacting multiple countries" if systems are breached.

Meanwhile, in the US, authorities have alerted companies to new malware targeting industrial facilities and systems that control machinery, and called on energy groups to harden their defences.

Vinnie Liu, co-founder of Bishop Fox, a cyber security testing company, reports a flood of inquiries from oil and gas companies since economic sanctions were imposed on Russia. Many have expressed concern that Russia will try to disrupt their operations, to increase dependence on Russia's own supply. "We are being asked to make sure the company is not a soft target," Liu says. "Companies are thinking 'Let's not be the one that gets hacked'."

Some hacks have been successful, though — and had real-world consequences. In late 2016, for example, Russia is believed to have been behind an attack that led to a power blackout in the Ukrainian capital of Kyiv. Others have been near misses. Last year, a hacker came close to poisoning the water in a treatment facility in Florida.

Energy plants are particularly vulnerable, though, because they rely on both IT systems and operational technology (OT), which can be older and harder to update. An electricity supplier cannot simply switch off a city's power while it upgrades its systems.

McKenzie notes that much of the energy sector is also catered to by local and regional providers, as well as a supply chain of third-party stakeholders with limited resources. "That's where there's still considerable risk," he says.

Cyber criminals are also joining nation-state hackers in this "lucrative" space, McKenzie adds.

As a result, energy companies need to ensure they are "bolstering intelligence and enhancing monitoring of usual suspects, watching for changes in [tactics] and hunting as they change", says Simon Hodgkinson, former chief information security officer at BP and a board adviser at the IT security group Reliance acsn.

Beyond the "basics" — which include updating and monitoring systems and having the necessary backups in place — energy companies need to undergo "crisis exercising", he says. "Prepare for the worst and ensure recovery and mitigation plans are robust."

Danielle Jablanski, an OT cyber security strategist at Nozomi Networks, says avoiding public panic when an attack takes place is essential, too. Social unrest can be as disruptive as an actual attack, and lead to unintended consequences.

Banks respond to digital threats after 'Pandora's Box' moment

OPINION

Kevin O'Rourke

When the global pandemic forced an almost overnight transition to remote working, it was a "Pandora's Box" moment for cyber crime: releasing malevolent forces into a newly vulnerable world of financial services.

Although the banking sector has always been a target for the criminal fraternity, remote working — which has now evolved into hybrid working — presented hackers with a more widely and thinly spread workforce to attack. At the same time, the onset of the pandemic prompted many organisations to reconfigure susceptible supply chains and offer more digital experiences. It did not take long for criminals to exploit any resultant vulnerabilities that these changes created.

Banks generally have complex interdependent supply chains with an array of financial technology and IT solution providers. So, when they all had to start operating differently, attackers could take advantage of this, and their approaches have evolved: not just stealing funds or sensitive data but extorting money by compromising servers, manipulating data, or even encrypting all of a victim organisation's data, using ransomware.

Together, all of these factors have created a surge in cyber crime activity within financial services — with attack methods becoming more sophisticated and targeted. For example, crime figures show that the number of credential and identity thefts have risen significantly.

Given the reputational damage a breach could cause, banks have developed robust practices to combat this threat. But there is also recognition that, while preventive actions are critical, it is still imperative for banks to know how to respond and recover from a cyber attack. They have therefore adapted disaster recovery and business continuity plans to specifically incorporate cyber incident simulation exercises — at both executive and operational levels.

Strategies have been developed that allow for full or partial recovery of the organisation's business critical services. These recovery plans are tested to ensure that all levels throughout an organisation are aware of their responsibilities during what could become a very stressed and time-critical event.

> Remote working presented hackers with a more widely and thinly spread workforce to attack

And it seems the industry has also recognised that, if it concentrates resources on innovation and digitalisation but fails to invest in cyber security and awareness, it is inviting trouble.

Consequently, it is becoming widely accepted that revenue generating concepts should be balanced with those allocated to respond to malicious cyber activity.

Banks are also paying much more attention to the risk exposure and resilience capabilities of their third- and fourth- party vendors.

These are some of the preventive measures that will be familiar to risk managers within the sector:

- **Data protection** Building system defences to protect sensitive information and intellectual property (the "crown jewels" concept);
- **Firewall protection** Enforcing connectivity restrictions to keep networks safe, in homes and offices;
- **Cyber hygiene** Maintaining the use of strong passwords and multi-factor authentication;
- **Antivirus software and back-up procedures** Investing in the latest technologies;
- **Phishing awareness** Familiarising staff with scams, and providing ongoing training on the constant threat from cyber criminals.

Kevin O'Rourke is group head of risk management for Bank ABC

ASSURED CYBER PROTECTION®

Humans & Technology, Intelligently Secure®

CYBER SECURITY IS NOT A TECHNOLOGY ISSUE

Talk to one of our experts about your cyber risk today

MAKE uk
The Manufacturers' Organisation

MAKE UK PROVIDING PRACTICAL SUPPORT AND INDUSTRY INSIGHT

Cyber Security

Make UK is at the forefront of helping organisations understand and manage the significant financial, operational and reputational risks posed by the increasing threat of cyber-crime.

We have partnered with Assured Cyber Protection, a leading cyber security services and solutions company, to deliver cyber services that meet the specific needs of our members, to help them understand and mitigate against current and future cyber security threats.

Get in touch today to find out how we can protect you.

makeuk.org/services/cyber-security

Why Make UK?

We're here to support you and your enterprise.

Providing access to HR & Legal, Health & Safety, Learning & Development, Cyber Security and wider expertise, Make UK provides essential knowledge and practical support to help your people and business thrive.

Our team of health, safety and sustainability specialists are on hand to help you maintain and develop a safe and healthy working environment.

Make UK Legal Services brings together a highly-qualified team of employment lawyers and HR specialists to give you the in-depth support you need. Combining the expertise and capabilities of a law firm with the practical experience of an HR consultancy, between us we have over 280 years' experience to back your business.

makeuk.org/services

Chain-driven: Toyota had to shut down its car plants in Japan after a suspected cyber attack on one of its suppliers — Shiho Fukada/Bloomberg

Smart factories need smarter IT

Manufacturing
Complex supply chains and connected machinery add risk, says *Sylvia Pfeifer*

Manufacturers suffered the brunt of cyber attacks last year, overtaking financial services and insurance as the most targeted sector. As the Covid-19 pandemic exposed the vulnerability of the long, complex supply chains favoured by global manufacturers, hackers bet on the ripple effects that disruption would cause for them.

More than 45 per cent of the attacks were on vulnerabilities that victim organisations did not, or could not, fix using software updates, according to IBM's latest Security X-Force Threat Intelligence Index.

These findings underline the increased threat to industrial companies as they grapple with the challenge of securing decades-old legacy systems.

Increasingly interconnected supply chains have only raised the stakes — with several global manufacturers reporting incidents. Earlier this year, Toyota shut down all of its plants across Japan after a suspected cyber attack on one of its suppliers.

Attacks are also increasing at a time when companies are integrating greater computing power, and more connectivity, into their production facilities.

So-called smart factories promise to improve quality and efficiency in manufacturing, as well as cutting response times. But they create new points of cyber vulnerability, especially if poorly implemented.

Manufacturers are "not as mature as the financial services sector, which has had these attacks for a number of years and is therefore ahead of the curve in terms of its protections", points out Del Heppenstall, cyber security partner at KPMG in the UK.

They are vulnerable to attacks on several fronts, too.

"From a ransomware perspective, manufacturers are quite exposed to time-driven critical processes, Heppenstall notes. "So, if you can cause a disruption, manufacturers are perceived to be more prone and therefore more likely to pay a ransom. Companies don't run dual manufacturing processes."

A further challenge for industrial companies is their reliance on what is often older technology to run the machinery in their manufacturing operations — whether that is making parts for a customer or building an entire product. Challenges arise when this operational technology is then connected to the company's corporate IT infrastructure.

All of these issues need to be addressed as manufacturers look to transform the way they operate to take advantage of interconnected systems and the "internet of things".

While a lot of research is going on into smart factories and what they should look like, the reality on the shop floor is still very different, warns Gareth Williams, vice-president of Secure Communications and Information Systems at French group Thales.

> 'If you can cause a disruption, manufacturers are perceived to be more likely to pay a ransom'

He says setting up a fully connected factory is not that simple, "unless you are building a brand-new greenfield factory from scratch".

A lot of clients, adds Williams, are in "that middle stage" — where they want to make the factory smart, to connect all their IT systems and make better use of the data but they have an "existing factory infrastructure that they spent many years and many millions of pounds building".

"Some of it is very old, some of it doesn't even recognise the internet," he explains.

While the question for larger companies is how they can protect themselves as they move along the path towards greater digitisation, the challenge for small and medium-sized companies is more often about getting the right level of support and expertise.

In its latest cyber readiness report, the UK-listed insurer Hiscox found that small- and medium-sized enterprises have borne the brunt of recent attacks. Companies with revenues of $100,000 to $500,000 now get as many attacks as those in the $1mn to $9mn bracket.

At the same time, however, IT spending by SMEs has fallen, leaving many exposed, the report reveals.

Ted Plummer, principal product manager at industrial 3D printing company Markforged, which counts companies from a wide range of industries among its customers, says SMEs and the "small machine shops are starting to realise how important maintaining around this digital thread is".

They need tools to "make it easy to be secure", he argues, because "people will do what is most convenient".

Leanne Connor, business manager at the National Digital Exploitation Centre in Wales, warns companies: "You are only as good as your weakest link."

The centre — a joint venture investment launched by Thales, the Welsh government and the University of South Wales — is situated on the site of a former steelworks in Ebbw Vale and provides training and support to companies to test and develop their digital concepts.

Connor says the key is to "get SMEs up to the right standard . . . the standards we expect from our supply chain are going up all the time".

KPMG's Heppenstall sees a "significant amount of third party supplier assurance taking place" as executives test the resilience of their organisations. "Continuity of service is just as important as data," he adds.

And, while digital transformation may be the ultimate goal for many, Heppenstall cautions that executives should not lose sight of what they are trying to achieve by going down this path. "We found a lot of companies start with the technology and work backwards to apply it," he says. "You should reverse the sequence and build the technology to meet the outcome you are looking to achieve by doing this digital transformation."

Travel sector Cyber attacks can be aimed at critical national infrastructure and customer data, explains *Nick Huber*

Transport: a moving target for hackers

Transport and travel groups are proving doubly attractive targets to cyber criminals — as both operators of critical national infrastructure, and as treasure troves of valuable customer data.

Over the past five years, cyber attacks on the IT systems and databases of transport organisations have increased and evolved, experts say.

In 2017, malicious software, or "malware", hidden in a document used to file tax returns infiltrated the IT systems of Maersk — and cost the global shipping company up to £300mn. A year later, hackers shut down 2,000 computers belonging to the Colorado Department of Transportation in the US.

And now, transport systems are seen as prime targets in international conflicts.

"There is some evidence from [US] government sources that nation-states and associated criminal organisations target lifeline [transport] infrastructure for cyber attacks more than other industries because these industries are strategically important to national security and the economy," says Bob Kolasky, a former assistant director at the US Cybersecurity and Infrastructure Security Agency.

Today, Kolasky is senior vice-president for critical infrastructure at Exiger, which advises companies on risk.

Meanwhile, fraudsters are hacking private travel companies' customer data. In 2020, easyJet discovered the email addresses and travel details of nine million customers were compromised, plus some credit card information.

Since then, both industries have reported a sharp increase in the use of ransomware (malware software that encrypts data to hold the owners to ransom), plus distributed denial of service attacks (which overwhelm a network or website with messages), as well as phishing (whereby cyber criminals pose as legitimate organisations to steal consumers' financial details).

In the case of transport organisations, attacks are typically mounted against IT systems, to cause maximum economic and social disruption to passengers and supply chains.

One of the vulnerabilities they face is the rudimentary nature of their "operational" technology – such as rail signalling, sensors, and port networks – when compared with state-of-the-art corporate IT systems.

Flight risk: airline computer systems are treasure troves of valuable customer data to cyber criminals — Evert Elzinga/Getty Images

"Operational technologies . . . can be disrupted by a hack, which can result in physical safety risks for people," points out Massimiliano Claps, research director and transport lead at IDC, a research company. "From that perspective, transportation is one of the industries that has one of the highest [cyber security] risk profiles."

And the areas of risk are widening, consultants warn. To automate maintenance and improve efficiency, transport companies are digitising their operational and external IT systems.

"[Operational] systems were never designed to be connected to other systems and never had security designed and built into them," notes Justin Lowe, a cyber security expert at PA Consulting.

In the case of travel companies, attacks tend to be focused on customer data, which can be financially valuable if sold on the "dark web" — hidden parts of the internet — and used for fraud.

Ross Henton, a former head of cyber security at American Express Global Business Travel, and now director at Mitiga, a cyber security technology company, says using this data safely must be a priority for travel groups. "One of the concepts we talk about in [cyber] security is the CIA triad: confidentiality, integrity, and availability," he says.

Fortunately, travel company IT systems are typically more advanced than those in the transport sector. But they contain more customer data, which creates different security risks.

Hospitality businesses are the third most targeted by cyber attackers of all industry sectors, behind retail and financial services, according to Trustwave's 2020 Global Security Report.

> 'Transportation has one of the highest risk profiles'
>
> Massimiliano Claps, IDC

Criminal groups attack hotel IT systems using methods including "spear phishing" (a targeted cyber attack against an organisation or individual) or they hack hotel WiFi, says Maximilian Heinemeyer, vice-president of cyber innovation at Darktrace, a cyber security technology company.

After breaching the hotel WiFi, a cyber criminal can install "keyloggers" – malware software on the victim's device that records everything they type and sends a log of the activity to the hacker.

Opportunities for customer data attacks exist because the quality of cyber security in hotels, airlines, and car rental companies varies. A further contributing factor is the extent of "interconnectivity" between companies' IT systems and the data, says Sherron Burgess, senior vice-president and chief information security officer at BCD Travel, a global travel agent for businesses.

BCD has responded to the threat by using "vulnerability management" technology to scan for security weak spots in its IT systems, and has adopted recognised cyber security standards, including ISO 270001. This stipulates that suppliers and trading partners follow minimum cyber security standards – including the use of firewalls and data encryption – and that security is checked regularly. "Anyone can do really well for one month," points out Burgess.

Regulators are also applying pressure. In the US, the Transportation Security Administration has issued directives requiring rail operators and pipeline companies to strengthen cyber security against ransomware attacks and other threats. They are also being made to implement a cyber security "contingency and recovery plan".

Similarly, the European Commission has published proposals to update and strengthen cyber security rules for network and information systems, which includes making senior managers accountable if their company fails to comply with the directive. This directive applies to travel companies, confirms Paul McKay, a cyber security and risk analyst at Forrester, a research company.

Cyber threats to travel and transport sectors are not expected to diminish, though, as the boom in ransomware continues, and as transport companies connect more industrial sensors and devices to the internet.

Operators are therefore advised to detect and resolve the risks — or at least minimise the damage of any security breaches — with standard cyber security software, staff training, and a well-rehearsed "incident response".

However, too often, companies in transport and travel take a "reactive" approach to cyber security and may only examine it after a breach, warns Henton of Mitiga. It may improve the situation in the short term, but "doesn't really [tackle] ongoing problems or drive cultural change", he says.

35% of manufacturers avoid cyber attacks due to enhanced protections

The rest suffer lost profits, lost revenues and lost customers

Uncover the secrets of success

Scan the QR code to read ACP's new report:
Five Habits of Cyber-Secure Manufacturers

ASSURED CYBER PROTECTION®

Humans & Technology, Intelligently Secure®

Hotels wary of unwelcome guests

Hospitality sector
Hackers see customer data as easy pickings, says *Alice Hancock*

Safety first: the Covid-19 pandemic has required hotels to store even more customer data and ensure it is secure — Pedro Fiúza/Getty Images

Hotels and hospitality businesses are now the third most targeted by cyber attackers of all industry sectors. Despite being bricks-and-mortar enterprises — set up for physical enjoyment of their amenities — they have become a rich mine of data for hackers with nefarious intentions.

Before Covid-19 forced hotels into a two-year period of on-off closures, they were the victims of 13 per cent of cyber compromises, according to Trustwave's 2020 Global Security Report — ranking just a little lower than retail and financial services companies.

And with hotels facing a difficult pandemic recovery and acute staff shortages, the increased use of technology to replace face-to-face services such as check-in and on-site payments has only raised this risk.

"Historically, hospitality has been a personal service, but I think they have started to realise that technology can facilitate a lot of that," says Tristan Gadsby, chief executive of hospitality consultancy Alliants.

What would previously, for example, have been an in-person chat or phone conversation, Gadsby notes, is now more often a virtual chat exchange. "We are seeing three times as many messages being sent post-Covid, compared to pre-Covid, per guest," he says.

In a sign of the times, the US commerce department last year issued its first set of guidelines for how hotels should secure customer data and critical software systems.

Meanwhile, authorities monitoring Covid's spread have also required more data from hotels — including their guests' contact details and health status.

Thomas Magnuson, founder of Magnuson Hotels, an umbrella company for hundreds of independent establishments, says his company tries to take minimal information from guests as "sometimes, when you travel, you feel like it is the biggest data grab of all time".

Hackers see international hotel chains, which process a huge volume of transactions, as easy pickings. Hotel groups also run valuable loyalty schemes with millions of members, who give up their data in order to earn points and improve their stays.

One of the most high-profile cyber incidents in recent times was the breach of Starwood's database in 2014, before the group was bought by Marriott, forming the world's largest hotel chain. That hack, which was only discovered after the deal, exposed the data of about half a billion customers, Marriott said, when it revealed the impact in 2018.

In a test case for Europe's then relatively new General Data Protection Regulation (GDPR), Marriott was fined £18.4mn by the UK data regulator, acting on behalf of the European Union — much less than the £99mn penalty originally threatened.

Marriott — which says in its privacy statement that it collects 15 different types of data throughout a guest's stay, from email addresses to passport information and preferred languages — has since "redoubled" its efforts "to detect and respond to threats", according to Arno Van der Walt, its chief information security officer.

The company sped up planned investment into data security and improved technology, such as software that detects suspicious cyber behaviour in real time, Van der Walt adds.

Yet hotels can be vulnerable to a range of cyber attacks, from ransomware to more specific intrusions, such as DarkHotel, a type of hack that targets high-level business guests through a hotel's WiFi network.

Luxury hotels are a particularly tantalising pool for criminals. In August 2020, scammers hacked into London's Ritz hotel's restaurant reservation system in an effort to convince guests to pass over their valuable payment details.

"The volume of data that [hotels] have is legend, therefore their data retention procedures need to be really up to scratch," stresses Fedelma Good, co-lead of PwC's data protection practice.

As cloud computing services have expanded, hotels have pushed more data storage towards external holders such as Amazon Web Services or Oracle — a move that at least means systems are being overseen by software experts, executives say.

> 'When you travel, you feel like it is the biggest data grab of all time'

Many hoteliers additionally employ third-party agencies to manage credit card details and keep different forms of data separate: "At the press of a button, I can tell what time [a guest] checked in, what time he left, what time he had lunch," says Sean McKeon, company secretary of Irish hotel group Dalata. "I have CCTV, but it's not all in one place."

However, staying safe does not come cheap for already cash-strapped hotels. Gadsby says running just one penetration test to find vulnerabilities in computer systems can cost up to $25,000.

Training staff is crucial. Several hotel executives point out that it is when staff are handling customer details that information is most likely to slip out.

"You wouldn't dream of appointing an executive head chef who didn't understand hygiene, so why would I appoint a head of marketing who didn't have an acute understanding of data protection?" asks McKeon. He says Dalata has spent tens of thousands on upgrading information security systems and training employees.

GDPR has forced companies to adopt much higher standards when it comes to data protection. But PwC's Good points out that for hotel groups with large cross-border footprints complying with regulations in every jurisdiction is "a real challenge".

Magnuson believes hotels should simply demand less data and not monetise it in vast loyalty programmes, as the big global chains do. Hilton, for example, raised $1bn during the pandemic just by selling advance loyalty points to its credit card partner American Express. "They talk about their millions of rewards owners and number of associated points [as] specifically valued assets," Magnuson observes.

And with guests demanding an increasingly personalised and individually tailored service, particularly from the well-known hotel brands, data is likely to remain a precious commodity in need of protection.

As Marriott expands online services — from phone notifications about when your room is ready, to using your mobile to unlock your door — Van der Walt says the company remains "laser focused" on the increasingly complex cyber environment: "This is a race that doesn't really have a finish line, hacks remain a threat."

ASSURED CYBER PROTECTION®

Humans & Technology, Intelligently Secure®

ARE YOU CYBER-SECURE?

People

A cyber-conscious culture is imperative for effective cyber security.

Organisation

Organisations that believe cyber security is a company-wide issue are more profitable.

Technology

When it comes to cyber-security protection, there is nothing without technology.

FT LIVE

Founding Partner

ASSURED CYBER PROTECTION

CYBER RESILIENCE SUMMIT

Navigating Risk in a Digitally Connected World

21-23 September 2022 | Beau-Rivage Palace, Lausanne, Switzerland

Nicole Perlroth
Former New York Times award-winning journalist and cyber security expert

Klara Jordan
Chief Public Policy Officer, *CyberPeace Institute*

Stephen Phipson
Chief Executive Officer, *Make UK*

Mitchell Scherr
Chief Executive Officer, *Assured Cyber Protection*

Edite Legere
Barrister, *One Crown Office Row*

Akshay Joshi
Head of Operations, *World Economic Forum's Centre for Cyber Security*

Alphonse Ibi Kouagou
Executive Director, *World Bank Group*

Public and private institutions around the world are facing imminent risk of cyber assault threatening national security, critical assets and business continuity. Now, more than ever, building cyber resilience is an urgent priority for leaders in business and government.

The exclusive gathering will unite CEOs, board members, government and policymakers to discuss strategies for overcoming new cyber threats which continue to threaten economic prosperity, national security and individual freedoms.

Expert speakers will share crucial insights on what can be learnt from recent cyberattacks, emerging risks, and how leaders can better collaborate on a unified response to cyber threats.

Register now at **cyber.live.ft.com**

For sponsorship opportunities please contact Peter Bamford at **peter.bamford@ft.com**
Stefan de Muynck at **stefan.de.muynck@consultants.ft.com**

Gold Sponsor

EY Building a better working world

Knowledge Partner

IMD

Pre-Dinner Drinks Sponsor

MAKE uk The Manufacturers' Organisation