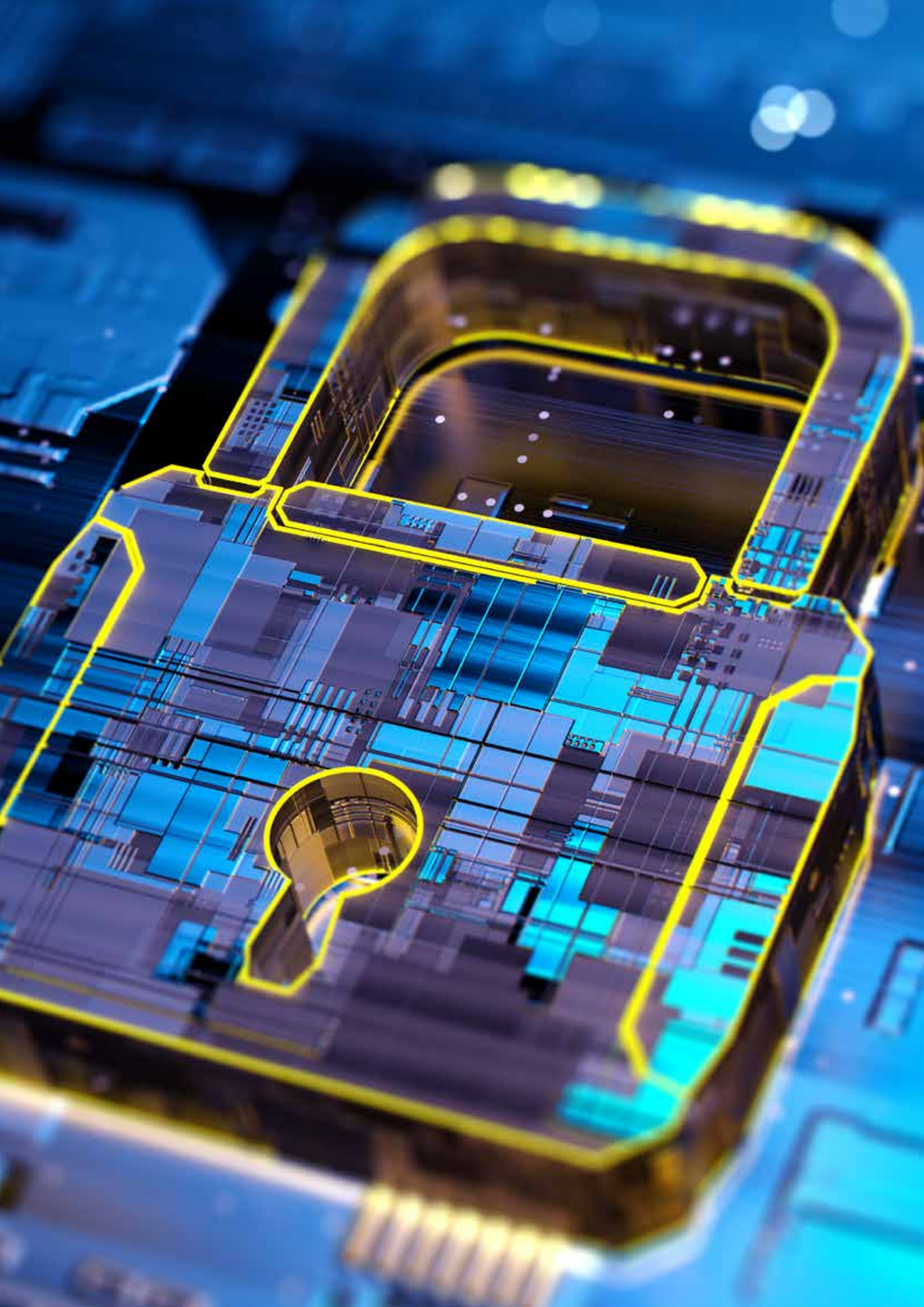
Are you equipped for the **challenge?**

A guide to cybersecurity leading practice in the equipment rental industry

EUROPEAN
RENTAL
ASSOCIATION

www.erarental.org


“Whilst much information exists globally on cybersecurity standards, technology and frameworks, this guide aims to offer latest insights and a “Roadmap” for good security and focused on our particular sector.”



A GUIDE TO CYBERSECURITY

Purpose of this guide

In 2021 our industry recognised that one of the greatest threats impacting it in the coming years was the vulnerability to cybersecurity impacts on our businesses. In 2023, this threat has increased due to global events, but also due to the intensification of the drive to “Digitalisation” across the industry globally.

In 2023, we continue to identify and communicate leading practice in cybersecurity that can support our industry, where an equipment rental company can evaluate where it stands in relation to cybersecurity and identify leading practice it can aspire to.

The purpose of the guide, first published in 2021 - and this version, the 2023 update - is to define the enterprise-wide scope of cybersecurity intervention, identify the core elements of a successful strategy, including the special factors that may impact rental companies, and to outline leading practices being adopted today by leaders in our industry.

This guide has been prepared by research with acknowledged leader companies in the equipment rental sector into practices in operation today to prevent and address cybersecurity vulnerabilities.

Whilst much information exists globally on cybersecurity standards, technology and frameworks, this guide aims to offer latest insights and a “Roadmap” for good security and focused on our particular sector.

THE GUIDE HAS BEEN COMPILED WITH THE INVALUABLE SUPPORT AND CONTRIBUTIONS OF ERA MEMBER COMPANIES, LED BY:

LOXAM
mateco YOUR BETTER WAY UP
renta
HSS Hire
RIWAL
Boels RENTAL
KILOUTOU
CGT A TESYA COMPANY
SUNBELT RENTALS
ARDENT HIRE SOLUTIONS
GSV
AvescoRent CAT Rental Store

The guide was prepared for ERA by DKR Projects Ltd, in conjunction with epi Consulting.
Images used in the guide are reproduced under licence (Deposit Photos Licence ID - OD-2297968) or from the iStock image bank.

GUIDE CONTENTS

01

The cybersecurity landscape for our sector

CYBERSECURITY
THE CALL TO ACTION

"There is nowhere to hide"

The equipment rental sector across Europe faces an unprecedented challenge in the threats posed by information technology vulnerabilities and exposures in our business.

The equipment rental sector across Europe faces an unprecedented challenge in the threats posed by information technology vulnerabilities and exposures in our business.

Customers are demanding more and more from us on cybersecurity protection. Our industry is in a process of consolidation for many reasons, but leaders stress that some of these drivers bring added cybersecurity risks; particular risks arise from smaller companies merging with others to achieve scale, larger companies acquiring smaller ones to enter new markets, to consolidate or win market share. The equipment rental business is embracing "Digitalisation". Hybrid working and more online interaction means more cybersecurity threats. Our equipment for rental is becoming more and more intelligent and more of it connected to networks, which can be the conduit for attack.

Today's cybersecurity threats are a **call to action** for all equipment rental companies, regardless of size, product or service type or geography.

No organisation is less likely to be a target for attack attempts than another. Everyone needs to play their part.

Equipment rental companies face all the threats that all industry faces, but they also need to deal with factors special to our types of business.

Equipment rental companies, who have experienced a serious incident, feel they have put their business, their reputation and, most importantly, their customers and stakeholders at high risk.

Everyone, *regardless of size and maturity in our industry,* is at risk.

> In 2021, ransomware attacks increased by 13%, a jump greater than the past 5 years combined. **Verizon**

> Corporate cyber attacks increased by 50% in 2021, when compared with 2020. **Cybersecurityintelligence.com**

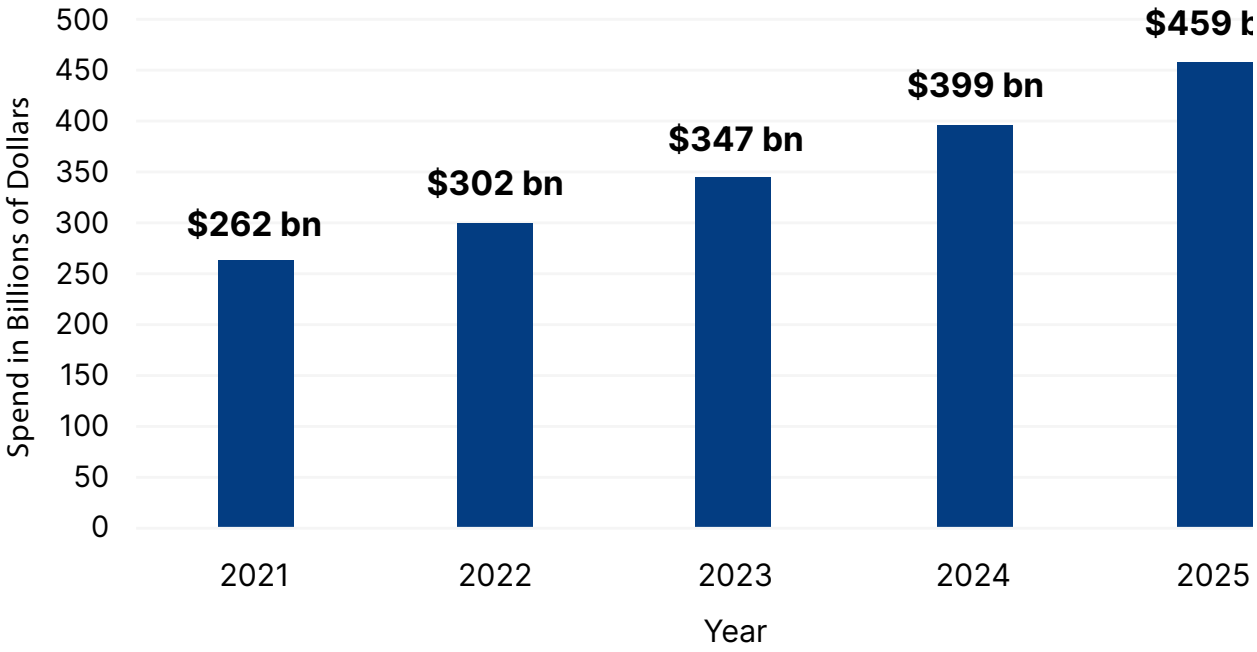
> The damage related to cybercrime is projected to hit $10.5 trillion annually in 2025, according to **Cybersecurity Ventures**.

> Where remote working was a factor in causing a breach, in 2021, the average cost was $4.96 million, that is $1.07 million higher than in breaches where remote work was not a factor. **IBM**

> 2021 illustrated how one key supply chain breach can lead to wide ranging consequences, where supply chain was responsible for 62% of System Intrusion incidents. **Verizon**

> Cybersecurity Ventures predicts that by 2031 there will be a new ransomware attack every 2 seconds. **Cybersecurity Ventures**

Global Cybersecurity Spending is predicted to reach $1.75 Trillion Cumulatively 2021 to 2025*



* Refer to: [cybersecurityventures.com - Spending 2021 - 2025]

> You may think you can stay under the radar, but the online intruders are smart and geared up with systems to scan for vulnerabilities. **There is nowhere to hide** – you have to work on the basis that you will be found... sooner or later.

CYBERSECURITY

THE THREATS FACING US TODAY

Cybersecurity threats

Equipment rental companies face all the same challenges as other sectors … but we also have *special* factors …

CYBERSECURITY THREATS REACH BEYOND OUR IT SYSTEMS. AREAS OF VULNERABILITY THAT ARE SPECIFIC TO OUR TYPE OF OPERATION INCLUDE THE UNEXPECTED VULNERABILITIES CAUSED BY CONNECTIVITY AND GPS COMMUNICATIONS. THESE INCLUDE VULNERABILITIES BETWEEN DIFFERENT INTERFACES (APIS), WHICH NEED FURTHER SECURING. THERE HAVE BEEN SERIOUS INCIDENTS IN OUR SECTOR, WHERE AN ATTACKER HAS, FOR EXAMPLE, USED A RENTAL COMPANY'S GEOLOCATION PLATFORM TO LOCATE STORED EQUIPMENT IN ORDER TO STEAL IT.

THE LAUNCH OF 5G OPENS DOORS FOR ADVANCED CYBER THREATS - THE HIGH SPEED OF DATA TRANSFERRING WILL ALLOW HACKERS TO INFECT MORE DATA PACKAGES AND SPY ON COMPANIES WITHOUT BEING NOTICED.

> **Email is the most common threat vector**, commonly used for phishing, malware and ransomware, but increasing sophistication and the use of other channels, like SMS phishing ("Smishing") are occurring.

> **Rental companies may be targeted on their own account or as a supply chain attack**, looking to infiltrate large national infrastructure customer systems and networks. During the COVID-19 pandemic, there was an increase in this type of attack, with attackers exploiting emergency home or remote working, where operatives may be using unprotected devices.

> **Attacks on vulnerable systems in a rental company** (including a reservation system, invoicing or even a preventive maintenance regime) that lead to compromise, or denial, of data can make it impossible to prove to customers that equipment is safe. This can lead to significant reputational damage and loss of business. Not only for the victim of the attack but across the sector.

> Equipment is increasingly dependent on connectivity, many through telematics, which are not always currently fully protected by equipment manufacturers in their build. **There is a need for more protection in equipment.**

"In July 2022, BitSight reported six severe vulnerabilities in a popular vehicle GPS tracker (MiCODUS MV720). Including allowing hackers to impersonate the true user via SMS, gain control and bypass the use of passwords. There are believed to be 1.5 million MiCODUS devices across 169 countries in use across various organisations. BitSight Discovers Critical Vulnerabilities in GPS Tracker"

"As a minimum, it should be more difficult for a hacker to crack our systems than the systems of others. Hackers will seek out the weakest first.

Many companies favour centralised and integrated systems architecture. But having decentralised IT systems can decrease vulnerability, as the attacker cannot gain control over the whole system.

Comprehensive and multilayer defence systems require significant investments from the company, which might not be appropriate to the level of risk involved. Systems, tailored to be fit enough for purpose, are best and should be matched to risk level individually by each organisation via a risk assessment across their estate."

CYBERSECURITY
SPECIAL FACTORS

An industry in consolidation

Customers are increasing their demands on us, their rental equipment providers, and we are increasing our demands on Original Equipment Manufacturers (OEMs) for constantly improving cybersecurity and evidence of preventive and protective practice. This is being driven by the drive to "Digitalisation".

The risk that hackers could gain access to national or large scale infrastructure operated by our customers, via a "back door" weakness originating from equipment rental is ever present. Leaders report that there are significant variations across Europe with countries and markets at different "speeds" in terms of what, and how much, customers require of their providers. Successful tender responses may require evidence for the customer that an equipment rental company operates a nationally or internationally recognised cybersecurity framework (*see "Roadmap" section*) or standards, particularly ISO 27001 or its equivalent. Conversely leaders report that, in general, the equipment rental sector can sometimes claim to be ahead of customers and OEMs in the race to improve cybersecurity. This in turn creates additional risks for us, given that an infiltration attack can occur at any point in the chain and move up or down it, so equipment rental companies must protect vertically up and down the supply chain, especially in data protection and sharing, as well as in the public domain.

SPECIAL FACTORS IN EQUIPMENT RENTAL MARKETS – CUSTOMER DRIVEN CYBERSECURITY?

Leaders point to the fact that, amongst all the special considerations creating additional cybersecurity risks, perhaps the single biggest factor is that the equipment rental sector is undergoing a turbulent period of consolidation with larger companies, acquiring smaller players and, in some cases smaller players merging together, and then being acquired.

In many instances, this rapid consolidation in the market has led to a lack of integration of systems and processes across acquisitions and leading practice now demands full integration into centrally protected system of these to avoid importing vulnerabilities into the weakest points of a newly combined organisation. Infiltration through a weak point is flagged as a major risk for entry by an attacker into an organisation's network "through the back door" and then onwards and upwards into their, and their customers', infrastructure.

Many leaders also point out that this risk is exacerbated when the acquisition strategy is focused on entry or growth in new markets, where (cybersecurity wise) processes and systems may be less mature than in the acquirer's home market.

“As a younger (five year old) equipment rental group, we had the opportunity to start from a zero base and approach IT security as a blank canvas. Given the special factors in the distributed nature of our industry, we found standard IT available didn’t always meet our needs so we took the strategic decision to **custom build systems** - and we still do. Likewise we had to custom build our cybersecurity from scratch but it gave us the opportunity to “design in” cyber safe features and forced an ethos that we will always consider cybersecurity needs in any new or changing IT system at design stage.

Since day 1, bringing people along with us was a matter of pragmatic common sense. We said to ourselves “You would not design a depot layout without a fence round it and strong locks on the gate. And it would have an intruder alarm system and cameras monitoring it. Why would you ever think it acceptable to design an IT system any differently?””

CYBERSECURITY THREATS

Equipment rental companies face all the same challenges as other sectors … but we also have special factors …

VULNERABLE TELEMATICS?

There have been a number of high visibility incidents involving the electronic hijack, mainly of road vehicles, over recent years as on board computing and network to vehicle communications grow in volume and sophistication. Much of the equipment in our sector carries telematics capability. Today, leaders do not typically consider such attacks as a clear and present danger, but it certainly could be a significant risk in the future and it should form part of a company's "Horizon scanning" for threats.

There are already reports of cyber attackers attempting to gain unauthorised control over heavy machinery via the remote control and monitoring systems. They could cause machinery to deviate from the execution plans with the intent of causing damage, or even injury, to those onsite.

Concerns have been raised that OEMs and equipment service companies are not yet doing enough to make telematics attack proof. Procurement decisions for new equipment should include an assessment to check that the models chosen are at the forefront of safety in telematics access and attack security. Increasing customer demands for data downloads via **telematics of equipment location and utilisation on site are thought to be the highest risk area**. Like all data sharing exercises, **single packets of carefully screened data, transmitted "one way" are considered safest**.

"We adopt the approach of minimising two way or live network communications of data between us and customers and other third parties. For GDPR (General Data Protection Regulation) and information security reasons, we make data downloads and transmission a "one way and one off" thing in each case, so as to avoid the risk of transmission and import of an infection."

> We are very aware that potentially large and dangerous types of equipment are open to attack, just as our own IT systems are. We need the OEMs to make the telematics as secure as they do the locks and alarms on the operating equipment itself. We evaluate and procure the “best in class” equipment we can, security wise.

> It's important to choose a secure telematics provider. One telematics provider was recently hacked - because every single device they built had a hard coded password of 123456.

Tech Tips: Telematics | For Construction Pros

> In 2019 Japanese security firm Trend Micro published a research paper demonstrating how it had been able to move full-size construction cranes by remotely taking control of radio frequency (RF) remote controllers. The researchers said that they were able to capture radio traffic and record RF packets which they could then replay to take control of the machine. This included replaying emergency stop commands indefinitely to produce persistent denial of service conditions. Hackers were also able to selectively modify the packets and craft new commands to completely control a machine.
>
> In January 2022, 19-year-old researcher David Colombo tweeted that he had been able to exploit security bugs in the TeslaMate logging tool to remotely hack into 25 Tesla cars in 13 different countries without the owners' knowledge, unlocking their doors and windows and starting keyless driving.

How to keep smart construction safe from hackers - Construction Europe

Leader strategy

RETAIL AND DEPOT OUTLETS AS "HUB OR SPOKE"?

Integration strategy is one of the most important areas of IT security focus for equipment rental Chief Information Officers (CIOs). They point to the fact that many operators have distributed operations with depots, compounds and retail outlets, often quite small, sometimes single person operations and they may well be geographically and internationally dispersed, compared to central operations.

These extended sites need to communicate with central networks in real time, but typically do so via mobile equipment, including smartphones, tablets and laptop computers. Where outlets have been acquired into the business, or are in less mature markets, they can be the weakest points in an equipment rental company's network and therefore an easier point of entry for an attacker than central systems would be.

Whilst leaders look to the retail and banking industries for models on how to protect distributed outlets, they note that our industry is fundamentally different, in that its outlets are typically low volume transaction nodes (perhaps a fraction of the volume of a typical supermarket, for example). This means that investment at sites in high bandwidth and secure fibre networks, in firewalls, encryption and High Security Modules (HSMs) needs to be substantial and may not always be justifiable in business terms but essential for cybersecurity.

"You have to protect data transmission and network connections to outlets. That means VPN tunnels to the centre, data transmitted to a "Sandbox" first and only then on to a firewalled data warehouse.

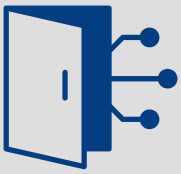
Strict standardisation and enforcement of the disciplines at a satellite location is key for us. We don't allow own devices to connect to networks, even use of the local hard disk on a laptop is against the rules. All storage is behind our firewalls on central servers."

LEADERS EMPHASISE THAT IT SECURITY STRATEGY HAS NO SINGLE RIGHT ANSWER FOR INTEGRATION BUT IT MUST BE SET CLEARLY THAT EITHER...

> the organisation will centralise and standardise protection and place each outlet at "arm's length" to its own firewall and security at point of sale **or**...

> it will incorporate all outlets within an overarching central firewall envelope. Either strategy can be effective, with reported advantages and disadvantages of each summarised below.

... **BUT** what is never right is "getting caught in the middle" with a mix of strategies.



"We believe in full integration of all acquired companies and outlets. We need to be advanced but not at any cost. There is no point spending money on cybersecurity central defence and millions more on an acquisition's and then "leaving the back door open" with vulnerable satellites."

CYBERSECURITY IN OUR INDUSTRY IS ALSO INCREASINGLY A LEGISLATIVE AND REGULATORY MATTER

EU legislation is centred around: "The Directive on Security of Network and Information Systems" ("The NIS Directive") and it is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

In May 2022, the NIS2 Directive agreement was reached. It updates the original NIS Directive due to the challenges of increasing digitalisation and interconnectedness (intensified by the COVID-19 crisis) and the rising number of cyber malicious activities at a global level.

NIS DIRECTIVE | SHAPING EUROPE'S DIGITAL FUTURE (EUROPA.EU)

THE ORIGINAL NIS DIRECTIVE PROVIDED LEGAL MEASURES TO BOOST THE OVERALL LEVEL OF CYBERSECURITY IN THE EU BY ENSURING:

- *Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,*
- *Cooperation among all the Member States, by setting up a **Cooperation Group** to support and facilitate strategic cooperation and the exchange of information among Member States,*
- *A culture of security across sectors that are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.*

THE UPDATED NIS2 DIRECTIVE ALSO INCLUDES:

- *Extended coverage, to include more critical entities across more sectors. Increasing the number of entities that are obliged to take cybersecurity risk management measures.*
- *Companies' cybersecurity requirements will be strengthened, by addressing supply chain and supplier relationships and accountability of top management.*
- *Streamlining of reporting obligations, introducing more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, and aims at harmonising sanctions regimes across Member States.*

Other areas of EU legislation are being developed that could impact the equipment rental industry's move to digitalisation, including equipment that uses telematics and software in many forms.

NEW MACHINERY REGULATION PROPOSALS

> The Regulations will include, amongst essential health and safety requirements, rules on security for connection and remote communication with the machinery and equipment types that are central to our industry.

> In order to pass the conformity assessment procedure, all these machines will need to have a certificate, issued under a relevant cybersecurity scheme.

> The new regulations are expected to come into force as early as 2023.

International Rental News: EU Machinery Regulation to impact rental

THE CYBER RESILIENCE ACT STATES TWO MAIN OBJECTIVES:

1. **Create conditions for the development of secure products with digital elements** by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and

2. **Create conditions allowing users to take cybersecurity into account** when selecting and using products with digital elements.

© European Union

Cyber Resilience Act | Shaping Europe's digital future (europa.eu)

02

Investment levels required

CYBERSECURITY IN EQUIPMENT RENTAL COMPANIES

INVESTMENT AND MATURITY

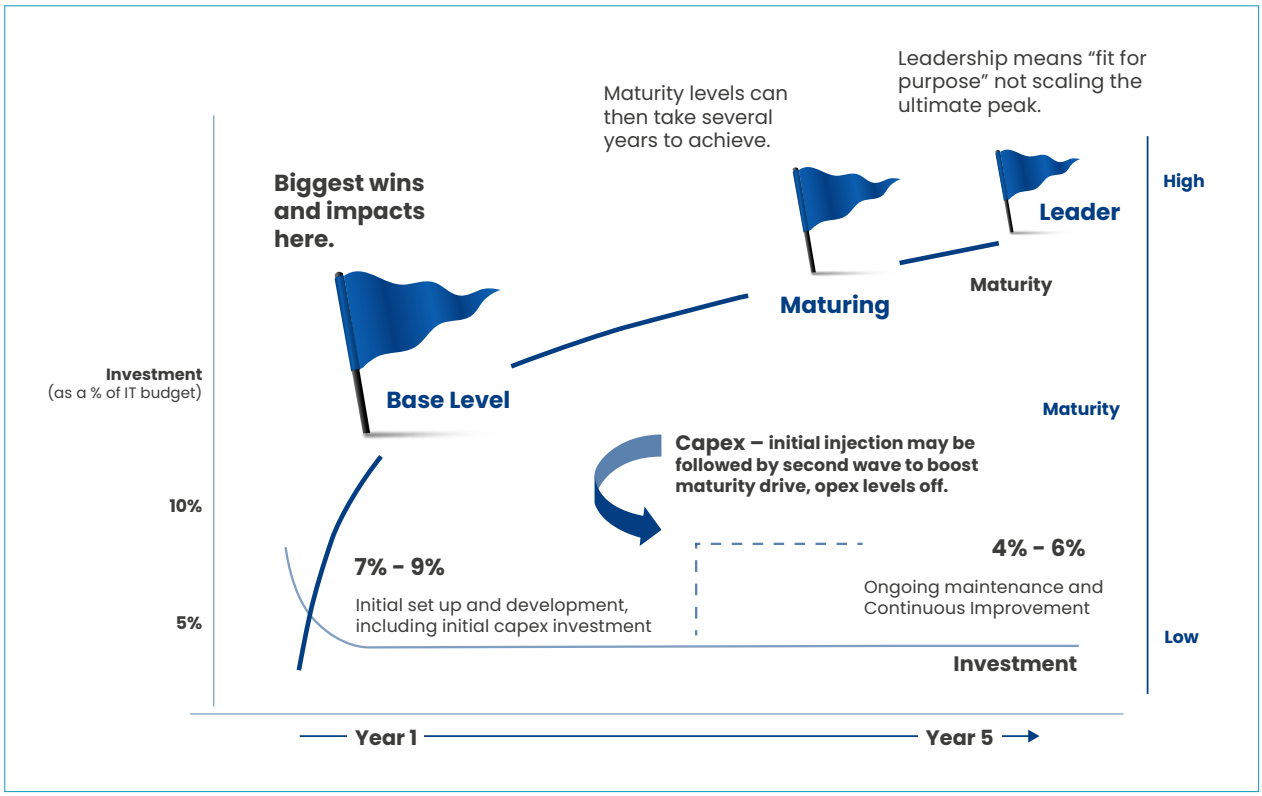
Special factors in equipment rental

HOW MUCH DOES CYBERSECURITY COST?

Good cybersecurity requires significant investment, renewed each year. A common benchmark for **direct** investment in cybersecurity across all industries is quoted as **4-6%** of IT spend.

They also stress that the larger investment is in **indirect and intangible** costs of "designing in", managing and embedding security into everything they do, which may ultimately be more than the direct costs.

But above all, the biggest progress and wins can come quickly at the start by low cost measures to get the basics in place:



LEADERS IN OUR INDUSTRY POINT TO THE FACT THAT COMPANIES AT THE EARLY PART OF THEIR JOURNEY MAY HAVE A MORE SIGNIFICANT "SET UP" COST (IF THEY ARE STARTING LOW DOWN ON THE MATURITY SCALE) - DEPLOYING PERHAPS 8% OF IT SPEND AT THE START - THEN SETTLING TO THE INDUSTRY NORMS OF 5% ANNUALLY TO SUPPORT MAINTENANCE AND ONGOING IMPROVEMENTS.

> The case for investment is not easy. The cost of avoiding a successful attack on the organisation is high, whilst the benefit of avoidance is invisible. Nonetheless the cost of a single breach can be millions of Euros, in a financially motivated theft - and we know it could actually be a terminal event for a business in a major service denial situation, so we justify our investments on that basis.

According to Gartner*, the typical split of budget spend (across all sectors) reflects the enterprise-wide need to protect all aspects of a business.

A company breakdown on average of a cybersecurity budget is:

> **Operational infrastructure security (48%):** Relates to general Network Security, Identity and Access Management (IAM), Privilege Access Management (PAM), Endpoint Security and all the activities involved in data security.

> **Vulnerability management and security monitoring (20%):** Relates to vulnerability assessments, vulnerability scanning, active discovery and remediation of vulnerabilities via ticketing, Security Operations Centre (SOC) performance and Security Information and Event Management (SIEM) costs.

> **Governance, Risk and Compliance (GR&C) (18%):** Relates to the active role involved in securing the company's data via an approved and certified framework, as well as complying with industry-specific regulations.

> **Application security (14%):** Relates to a combination of penetration testing practices geared towards improving hardware, software and employees from a running list of evolving threats.

Leaders also stress the strong link between cybersecurity investment and reducing risks of GDPR (General Data Protection Regulation) penalties.

> The EU GDPR sets a maximum fine of €20 million) or 4% of annual global turnover – whichever is greater – for infringements, involving loss of data.

*Refer to: **NIS Investments 2021 (ENISA Report)** – trends quote in the report are presented through Gartner security data and insights observed globally.

Business email compromise (BEC) was responsible for only 4% of breaches, but had the highest average total cost of the initial attack vectors, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million)

IBM ***also reported that, in 2021, the 4 most common causes of data breach by initial attack vector were:***

> 20% - Weak and stolen credentials (passwords)

> 17% - Phishing

> 15% - Cloud misconfiguration

> 14% - Vulnerability in 3rd party software

IBM

THE COST OF VULNERABILITY

A 2022 Gartner survey shows 88% of Board of Directors regard cybersecurity as a business risk rather than solely a technical IT problem.

Gartner predict that by 2025, 60% of organisations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements **Gartner.**

In 2021 it took an average of 212 days to identify a data breach and an average 75 days to contain it, with breaches caused by stolen/compromised credentials taking the longest to identify (250 days) and contain (91 days) **IBM**.

03

Cyber insurance

THE CASE FOR CYBER INSURANCE

Cyber Insurance - To have it or to not have it?

- Many rental companies report that they do currently have a policy of having cyber insurance, but not all.
- It is often perceived as increasingly expensive, given the trend of increasing threat and with reducing cover scope or level of cover.
- Those who don't have it, don't necessarily see the need for it and do not intend to adopt it in the foreseeable future.
- Most of those who do have insurance consider it as a part of a standard scope of company or group insurance requirements, rather than something they seek to secure as part of their security strategy.
- Some, but not all, markets, are seeing (corporate) customer requirements for rental companies requesting evidence that they have cyber insurance in addition to public liability or similar cover.
- Those members who formed part of a larger group felt that cyber insurance was a "group level" matter and so afforded them better support than being standalone.
- Applying for insurance is onerous, with most members reporting insurers requiring end to end risk assessment and maturity analysis prior to quote. This content can be 200 items plus and usually non standard, i.e. custom built assessment forms, differing by insurer.

> "The average duration of damage being wreaked by a serious and successful attack is 267 days... but you may not even know you have it until well into that period."

WE FACE THE CHALLENGES OF AN INSURANCE INDUSTRY IN TURMOIL WHERE THE CYBER INSURANCE PRODUCT IS IN FLUX, PERCEIVED AS INCREASING RISK TO THE INSURER, WITH A TREND OF EXPONENTIAL INCREASES IN PREMIUMS AND REDUCTION IN COVER SCOPE AND SUMS INSURED.

> We have insurance, but we wouldn't rely on it in the event of an incident.
>
> Cyber insurance is expensive, because cyber attacks are expensive. It is one of those parts of a business that requires such a level of financial cover that being part of a group, or being acquired by a bigger group, may be the first time you get the peace of mind that you could afford a major attack and resume business successfully afterwards.

THE CYBER INSURERS' PERSPECTIVE:

Smaller companies are often "cyber novices" and ...

... THERE IS A BIG DIVIDE BETWEEN LARGE AND SMALL.

Average spending by firms with 250 to 999 people has doubled in the past year. For enterprise firms of 1,000-plus it is up 65%.

...At the other end of the scale it is a different story. Firms with between 10 and 49 employees have almost halved their cybersecurity budgets. Among those with under 10 employees, spending has collapsed – from an average of $150,000 to just $29,000.

CONTRACTED-OUT CYBER DEFENCE?

Some member SMEs acknowledged they have limited cyber knowledge and involvement.

This a specialised area and so they "contract out" systems and support to IT service providers, particularly for cloud, network, VoIP and office systems, which is perceived to bring with it an advanced level cyber defence than they would achieve in-house.

The Hiscox Cyber Readiness Report provides a unique gauge of the state of commercial cybersecurity across eight markets in Europe – the UK, the US, Spain, the Netherlands, Germany, France, Belgium and Ireland.*

*The Hiscox Cyber Readiness Report 2022 | Hiscox UK

Ransomware rises
19% of respondents reported a ransomware attack, up from 16%.

Two-thirds of the firms paid up.

More cyber policies
64% of companies now have cyber insurance as a standalone, or part of another, policy. Up from 58% two years ago.

Increased spending
Respondents' mean cybersecurity spending is up 60% in the past year to $5.3m, and has increased by 250% since 2019.

"We are not in favour of paying ransoms. If you pay, the criminals have you "dialled in" and are back again six months later for more.

They are still in your network, just waiting to push the attack button again.

If you think the insurance company will reimburse you, if you pay the ransom ...think again."

INSURANCE INDUSTRY VIEW

There is a call to action for the "cyber novice"

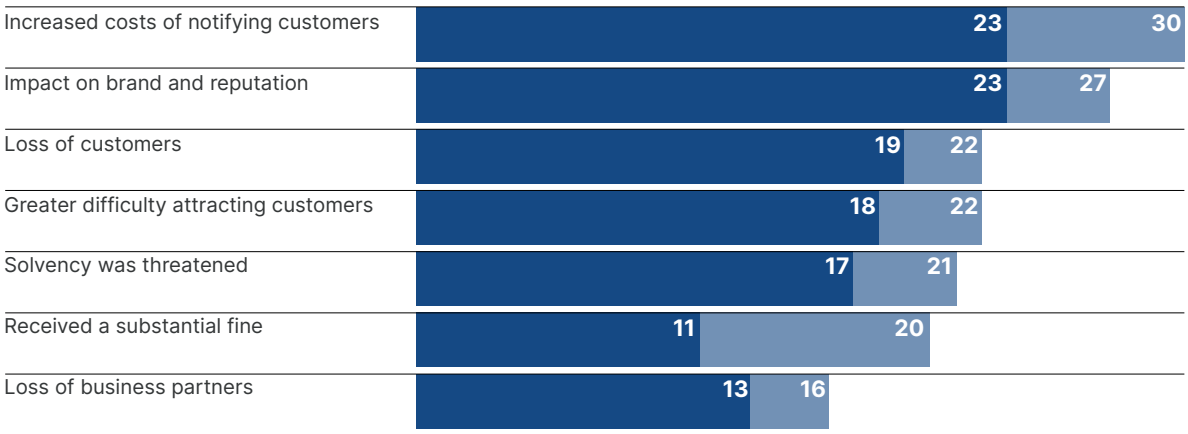
The insurance industry confirms what we are seeing in our in-industry interviews and polls - there is lower cyber maturity and lower uptake typically amongst smaller companies, who are described as "**cyber novices**".

Firms who have been attacked are twice as likely as others to seek cyber insurance

WHILST CYBER INSURANCE MIGHT TYPICALLY PROVIDE DIRECT COST COVER, CUSTOMER AND BRAND DAMAGE MAY BE THE BIGGER COST IN RAPIDLY DIGITALISING MARKETS

Effects of a cyber attack (%)

The effects of a cyber attack go well beyond the direct financial consequences.
More businesses are discovering that there is increased impact across the board.



While big businesses have been investing ever more in building cyber defences, spending by smaller firms has fallen sharply this year. That appears to be part of a decline in overall IT spending at the lower end of the corporate spectrum. But this is not coming at a good time.

The Hiscox Cyber Readiness Report provides a unique gauge of the state of commercial cybersecurity across eight markets in Europe – the UK, the US, Spain, the Netherlands, Germany, France, Belgium and Ireland.*

*The Hiscox Cyber Readiness Report 2022 | Hiscox UK

ON THE OTHER HAND, THE INSURANCE INDUSTRY REPORTS THAT ...

> January 2022: Gartner predicts that within three years, 80% of the magnitude of fines imposed by regulators after a cybersecurity breach will be attributable to failures to prove the duty of due care was met rather than the impact of the breach.

gartner.com

MATURITY IN CYBERSECURITY IS STILL LARGELY THE PRESERVE OF LARGER COMPANIES WITH THE ABILITY TO INVEST, BUT "SUNRISE" RENTAL COMPANIES AND THOSE DRIVING DIGITALISATION ARE EXCEPTIONS

Smaller rental companies clearly recognise the risks arising from cyber threats, and increasingly over the last three years but are only now getting ready to act.

KEY DRIVERS FOR THE CALL TO ACTION ARE GROWING:

> The increased scope of telematics in equipment is rapidly creating new cyber risks and the spectre of active hijack or sabotage of equipment with human injury consequences.

> The changes in ways of working and the continuation of distance working brought about by the Covid pandemic means more remote resilience and practices.

> The perceived increase in cyber threats globally, some related to the Russian conflict in Ukraine. (These appear more pronounced in smaller rental companies, where cyber defence is often less prepared and robust).

> In the rental industry as well as outside it cyber maturity is a size and scale play, where larger budgets allow sizable cyber defence investment.

> Those newer "sunrise" rental companies, who show all the characteristics of being "digitally native", consider their business models, systems and processes to have cyber defences built in.

THERE ARE EXCEPTIONS:

> Those who have suffered an attack are twice as likely to have taken measures and taken on cyber insurance.

> Those who take on shared cyber and IT services from a third party expert provider consider it a form of insurance, which reduces their perceived exposure and risk.

> "There is a drive in some of our markets (predominantly UK now but spreading) for (large) rental customers to require supply chain (often smaller) companies to declare formal cyber qualifications and evidence insurance cover.
>
> There is no point in our customers cyber proofing their own operations and allowing suppliers to be weak."

CYBER INSURANCE

To have it or not to have it?

ON BALANCE

- Where an organisation has **extensive insurance cover as a core strategy across the business**, it makes sense to include cyber insurance in scope.
- Where organisations have **high levels of cyber maturity** already, insurance is more affordable and more likely to pay out in the event of a claim.
- In some markets, **"ticking the cyber insurance box"** for customers can increasingly be a business enabler.
- Where the cover includes "emergency assistance " with pre-approved budget or similar fast response features, **insured companies feel the insurance can really add value**.

- **Cover offered is increasingly exclusions driven.**
- Pre-qualification and terms of cover are being **tightened**.
- Very few members had confidence that the insurance would be of use in the event of **an attack or a subsequent claim**.
- A number of instances were outlined that months or a year or more after an event a claim was still being investigated or challenged by an insurance company, sometimes with legal advice being required on both sides. In some cases claims were being abandoned part way through due to the **overhead cost of pursuing the claim**.

> Cyber insurance is expensive, because cyber attacks are expensive. It is one of those parts of a business that requires such a level of financial cover that being part of a group, or being acquired by a bigger group, may be the first time you get the peace of mind that you could afford a major attack and resume business successfully afterwards. What price is survival worth?
>
> ... Many of the rental companies who hold insurance report that the features of some policies, such as having a pre-approved budget for emergency or specialist third party support to triage or defend an attack, is very valuable.

> We're seeing that the proposed cost of insurance would now be more than our total security budget. That makes no sense.

> Insurers only want to cover risks that are unlikely to happen, for example, this year our cover scope excluded Ransomware attack. The message from insurers is "No MFA (Multi Factor Authentication), no insurance". There are clear red lines developing, one is MFA.

> The more difficult part is that insurers seek to exclude human error, so if you confirm on the policy evaluation that your staff will always keep all your PCs updated without exception, then you will probably need to prove it in a claim. Few of us can demonstrate perfection.

CYBERSECURITY BENCHMARKS

This guide defines a maturity pathway and aligns with the KPIs that insurers are often asking applicants to report and evaluate

CYBERSECURITY WITHIN EQUIPMENT RENTAL COMPANIES ENTERPRISE-WIDE'' INTERVENTION *(see page 54)*

CUSTOMERS

PROCESS

- Cybersecurity Plan and Investment
- Risk Assessment
- Industry Frameworks and Standards
- Governance
- Continuous Improvement and Horizon Scanning

TECHNOLOGY

- Inventory Management
- Firewall Management
- Secure Configuration
- User Access Control
- Malware protection
- Security update management
- Distributed Networks
- Threat and Health Monitoring

STAKEHOLDERS

PEOPLE

- Enterprise-wide Awareness
- Training and Development
- Roles and Responsibilities
- Monitoring and Coaching
- Cybersecurity Personnel - Roles and Responsibilities

INFRASTRUCTURE

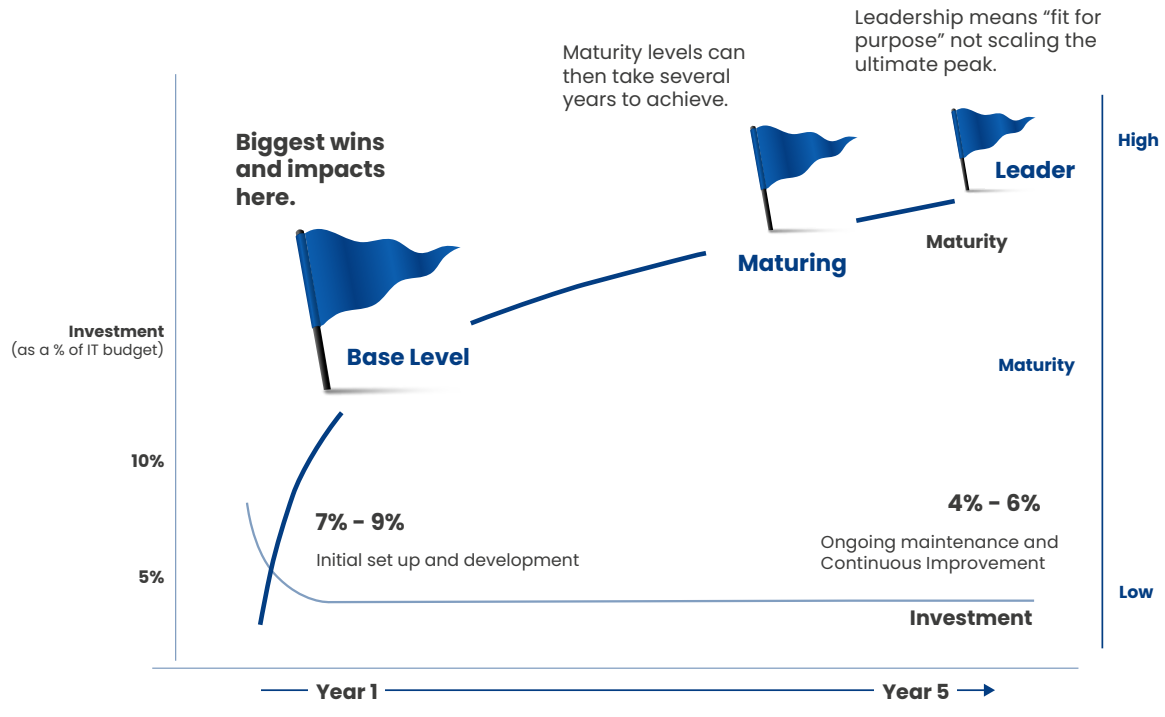
- Policies and Procedures
- Communications
- Emergency Response
- Customer Management
- Supply Chain Management
- Maintenance

CYBERSECURITY BENCHMARKS - COST BENCHMARKING - UNDERSTANDING COST OF COMPLIANCE/NON-COMPLIANCE

The guide considers key factors in "Investment and Maturity"

> Good cybersecurity requires significant investment, renewed each year. A common benchmark for **direct** investment in cybersecurity across all industries is quoted as **4-6%** of IT spend.

> Larger investment is in **indirect and intangible** costs of "designing in", managing and embedding security into everything they do, which may ultimately be more than the direct costs.



THE GUIDE DETAILS EACH "MATURITY STAGE" BY ELEMENT AND OFFERS A TEMPLATE FOR A RISK ASSESSMENT *(see page 56)*

Features of each maturity level:

PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

ELEMENT	BASE LEVEL
Cybersecurity Plan and Investment	Full "Asset Inventory" and map of vulnerabilities created. Highest priority fix areas planned and budgets set. Cybersecurity goals and targets roadmap set.
Risk Assessment	High, medium and low risks identified enterprise-wide. Action plans for highest priorities set.
Industry Frameworks	Target Framework and Standard(s) (or equivalent in-house Framework identified. "Base level" achieved in chosen Framework(s), (such as "cybersecurity Essentials,*" or CIS: "Basic CIS Controls** level.
Governance	Key governance issues and reporting processes identified. Strategic players to form governance group in organisation identified.
Continuous Improvement and Horizon Scanning	Awareness of latest threats and anticipated future trends, to feed into base level planning.

Analysis by factor then feeds into a risk assessment

MATURING	LEADER	KPIs
Base level risk mitigation and priorities implemented. Analysis of next 3 years' priorities in place and investment plan set. Cybersecurity plan integrated into overall IT and Business Plan.	Enterprise-wide plan, with five year horizon, refreshed annually. Investment plan for maintenance and continuous improvement in operation.	Compliance to plan and target "Milestones"
Risk and mitigation overarching plan defined and corresponding investments approved. All high risk vulnerability actions implemented.	All risks addressed or mitigated. Annual or more frequent refresh of risk assessment process in place. Periodic risks audit function in place.	Number and percentage of risk threats addressed, number outstanding versus plan
Advanced or "Maturity" level achieved in chosen Framework(s), demonstrating all vulnerabilities are covered and monitoring is in place (such as "Cybersecurity Essentials, Plus*" or "Foundational CIS Controls**" level.	Achievement of high level of maturity in chosen Framework(s), (such as CIS: Organisational Levels and/or ISO 27001).	Achievement of plan level, or equivalent. Compliance audit pass/fail and exceptions
Governance process in place and operational. Co-ordination of reporting to board on strategic health implemented.	Governance fully integrated into business management and managing cybersecurity plan outputs and investments.	Strategic Health monitor report outputs. Compliance to plans, testing and audits.
Governance forum carrying out horizon scanning (reviewing latest published reports and bulletins from bodies involved in IT Security worldwide) and periodic review of improvements to critical processes.	Continuous improvement and horizon scanning processes fully integrated into governance. Bulletins and alerts integrated as part of communications activity.	Reports and bulletin outputs.

ERA Cybersecurity — Company checklist for Intervention Priorities

Capability Element	Maturity level today			Risk Level			Priority for Action
	At or below Base level	At or nearing mid-level maturity	At Leader level	Low	Med	High	1,2,3
PROCESS							
Cybersecurity Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement/Horizon Scanning							
Other?							
PEOPLE							
Entreprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							

04

Roadmap of leading practices and “Checklist”

ENTERPRISE-WIDE CYBERSECURITY

SCOPE OF INTERVENTION FOR EQUIPMENT RENTAL COMPANIES

This guide offers a model and template across the four main areas of a business of our type to scope out, risk assess and prioritise interventions to optimise cybersecurity strategy.

All companies are different, all at different stages, all with different needs and budgets and many following adopted frameworks and strategies, but we hope this model, compiled from combined experiences of leaders in our sector may be a useful "Roadmap" for those at base levels and a "Checklist" for those maturing their security to ensure all areas are covered.

Leaders emphasise that, whilst a comprehensive security plan forms an essential part of an overall business strategy, "an over-arching plan" does not have to be the very first step - a full plan may typically come in maturity stages. It is most important in early stages to take steps to identify all possible high risk areas in the business and prioritise actions to plug or patch vulnerabilities.

A comprehensive scan of risks across each of the four elements outlined in this guide as a checklist can be a good starting point. As high risk areas are dealt with, medium areas can then be tackled. It is important to say that research indicates that, from a base level, moving up to cover all significant risk areas to leader levels, can be a three to five year process, requiring material and sustained investment. Each organisation should do what is appropriate to the risk assessment of their security – not necessarily "to reach for the stars".

A checklist for scope, risk assessment and prioritisation based on the four elements in the roadmap is included as a useful template see page 64.

ERA Cybersecurity — Company Checklist for Intervention Priorities

Capability Element	Maturity level today			Risk Level			Priority for Action
	At or below Base level	At or nearing mid-level maturity	At Leader level	Low	Med	High	1,2,3
PROCESS							
Cybersecurity Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement/Horizon Scanning							
Other?							
PEOPLE							
Entreprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							
Monitoring and Coaching							
Cybersecurity Personnel - Roles and Resp's							
Other?							
TECHNOLOGY							

"You get what you measure..."

Leaders report that it is essential to ensure key areas of performance that impact your cybersecurity status are measured with Key Performance Measures (or Indicators) (KPIs) in place. The roadmap in this guide also indicates typical measures and performance measurement systems in use today by leader companies.

The focus for cybersecurity interventions is often around technology and systems. However, many risks have root cause in human behaviour, robustness of processes and monitoring, reporting and responses within the enterprise.

According to equipment rental leaders in this field, an organisation needs to consider an enterprise-wide strategy to ensure all areas of vulnerability are considered.

Each organisation will have different risks, scope of operations and gaps, however leaders consider that a checklist for a comprehensive scope can be captured under four capability elements covering:

> PROCESS

> PEOPLE

> TECHNOLOGY

> INFRASTRUCTURE

WHILST EACH COMPANY WILL HAVE DIFFERENT APPROACHES AND PRIORITIES, THIS FOUR FACTOR MODEL PROVIDES AN ENTERPRISE-WIDE "CHECKLIST" OF ELEMENTS TO CONSIDER...

CYBERSECURITY WITHIN EQUIPMENT RENTAL COMPANIES

"ENTERPRISE-WIDE" INTERVENTION

CUSTOMERS

PROCESS

> Cybersecurity Plan and Investment
> Risk Assessment
> Industry Frameworks and Standards
> Governance
> Continuous Improvement and Horizon Scanning

TECHNOLOGY

> Inventory Management
> Firewall Management
> Secure Configuration
> User Access Control
> Malware protection
> Security update management
> Distributed Networks
> Threat and Health Monitoring

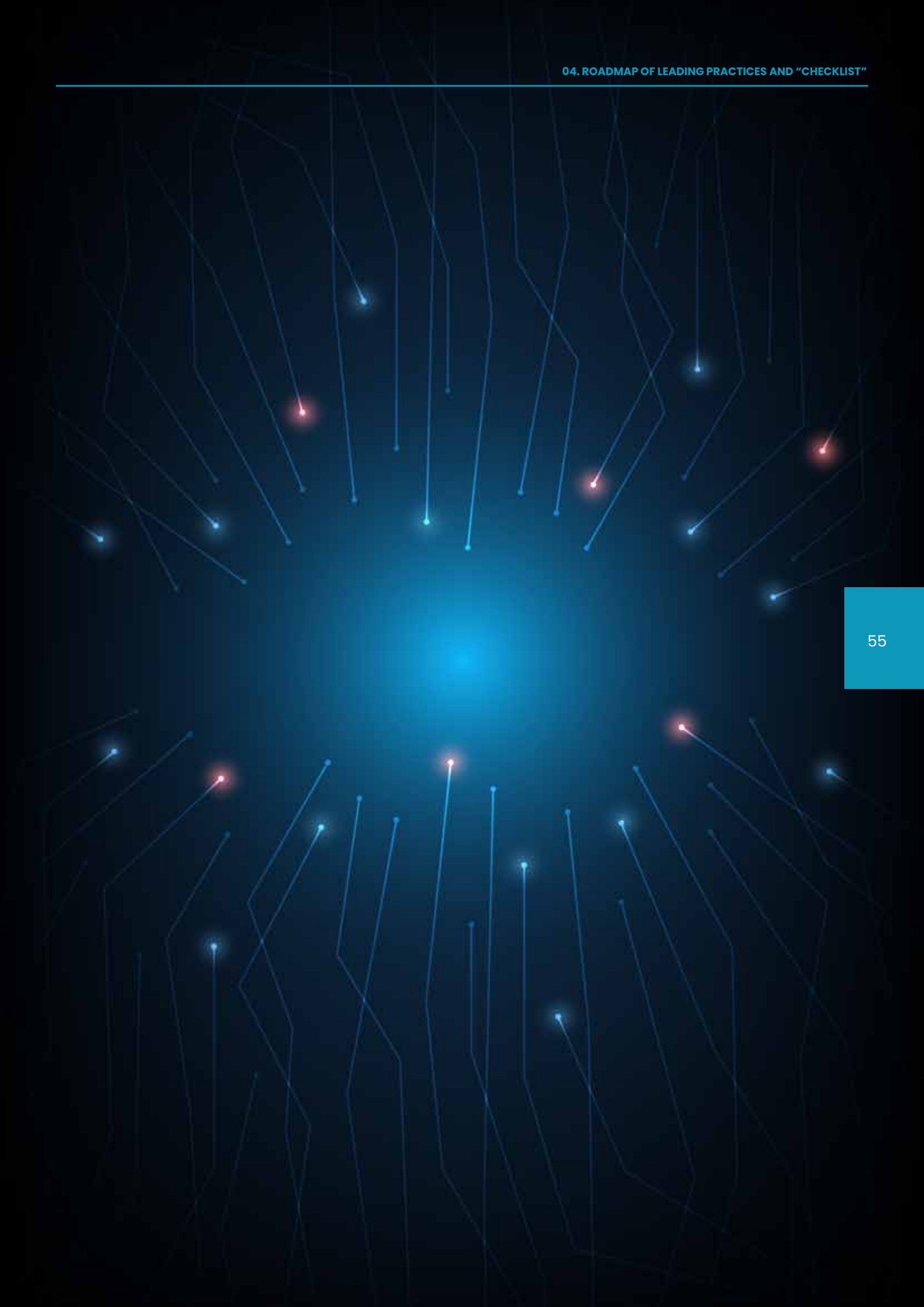
STAKEHOLDERS

PEOPLE

> Enterprise-wide Awareness
> Training and Development
> Roles and Responsibilities
> Monitoring and Coaching
> Cybersecurity Personnel - Roles and Responsibilities

INFRASTRUCTURE

> Policies and Procedures
> Communications
> Emergency Response
> Customer Management
> Supply Chain Management
> Maintenance



CYBERSECURITY IN EQUIPMENT RENTAL COMPANIES

MATURITY STAGES

Features of each maturity level:

PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

ELEMENT	BASE LEVEL
Cybersecurity Plan and Investment	Full "Asset Inventory" and map of vulnerabilities created. Highest priority fix areas planned and budgets set. Cybersecurity goals and targets roadmap set.
Risk Assessment	High, medium and low risks identified enterprise-wide. Action plans for highest priorities set.
Industry Frameworks	Target Framework and Standard(s) (or equivalent in-house Framework identified. "Base level" achieved in chosen Framework(s), (such as "cybersecurity Essentials,*" or CIS: "Basic CIS Controls** level.
Governance	Key governance issues and reporting processes identified. Strategic players to form governance group in organisation identified.
Continuous Improvement and Horizon Scanning	Awareness of latest threats and anticipated future trends, to feed into base level planning.

Also see section on "Leading practices examples– Process"

*Refer to: **About Cyber Essentials - NCSC.GOV.UK**

**Refer to: Cybersecurity Best Practices (cisecurity.org)

MATURING	LEADER	KPIs
Base level risk mitigation and priorities implemented. Analysis of next 3 years' priorities in place and investment plan set. Cybersecurity plan integrated into overall IT and Business Plan.	Enterprise-wide plan, with five year horizon, refreshed annually. Investment plan for maintenance and continuous improvement in operation.	Compliance to plan and target "Milestones"
Risk and mitigation overarching plan defined and corresponding investments approved. All high risk vulnerability actions implemented.	All risks addressed or mitigated. Annual or more frequent refresh of risk assessment process in place. Periodic risks audit function in place.	Number and percentage of risk threats addressed, number outstanding versus plan
Advanced or "Maturity" level achieved in chosen Framework(s), demonstrating all vulnerabilities are covered and monitoring is in place (such as "Cybersecurity Essentials, Plus*" or "Foundational CIS Controls**" level.	Achievement of high level of maturity in chosen Framework(s), (such as CIS: Organisational Levels and/or ISO 27001).	Achievement of plan level, or equivalent. Compliance audit pass/ fail and exceptions
Governance process in place and operational. Co-ordination of reporting to board on strategic health implemented.	Governance fully integrated into business management and managing cybersecurity plan outputs and investments.	Strategic Health monitor report outputs. Compliance to plans, testing and audits.
Governance forum carrying out horizon scanning (reviewing latest published reports and bulletins from bodies involved in IT security worldwide) and periodic review of improvements to critical processes.	Continuous improvement and horizon scanning processes fully integrated into governance. Bulletins and alerts integrated part of communications activity.	Reports and bulletin outputs.

PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

ELEMENT	BASE LEVEL
Enterprise-wide Awareness	Briefing out of all main security related policies and procedures to all personnel, both centrally and in the field has taken place and update schedules set.
Training and Development	Relevant first and second line populations, requiring training identified and training needs set.
Roles and Responsibilities	First and second line staff roles and responsibilities, within day to day security context, identified and added to core role descriptions.
Monitoring and Coaching	Using high priority risk assessment, all staff in high risk areas or failing base level training, given individual coaching and "retesting"
Cybersecurity Personnel - Roles and Responsibilities	Appointment of Security Officer(s). Training and development plans for specialist security skills identified. Role descriptions for specialist roles and responsibilities for security staff in place

Also see section on "Leading practices examples – People"

MATURING	LEADER	KPIs
Awareness briefing updates schedule implemented. Internal channels in place to broadcast news on cybersecurity related updates, changes and new threats	"Two way" feedback forums in place to contribute to continuous improvement.	Active use of media and comms channels.
Training qualification and certification schemes for each level set and rollout in place. Security personnel accredited.	All first and second line staff trained. Further education and development plans in place for key staff.	Training hours delivered; training hours per staff member.
All staff roles and responsibilities identified and added to role descriptions. Emergency response special responsibilities defined and implemented with key responder staff.	Management and Board roles and responsibilities in place with cultural acceptance of cybersecurity roles ("Walk the Talk").	Percentage of staff with defined day to day special responsibilities in cyber de-fence added to their roles.
Penetration testing and "Phishing" simulations to test competencies for first line staff.	Penetration testing and "Phishing" simulations to test competencies for all staff.	N°. of incidents or successful attacks with human error factor.
Security Officer(s) actively integrated into organisational design enterprise-wide, (not just IT department). Reporting mechanisms and forums in place, managed by security department.	Security personnel actively monitoring and horizon scanning for new initiatives and leading continuous improvement initiatives.	Number of dedicated staff or man-hours to cy-bersecurity as a proportion of overall staff resources and IT hours/costs.

PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

ELEMENT	BASE LEVEL
Firewall Management	Firewalls established at the boundary between network and internet of all high and medium risk systems and devices.
Secure configuration	All high and medium risk systems passworded or code locked - default passwords changed. Non essential programmes and software deleted.
User access control	Non essential user accounts deleted. Audit of existing user access carried out. New user set up and access approval process in place.
Malware protection	Anti-malware software installed on high and medium risk systems and devices. Malware warning alarms activated.
Security Update (Patch) Management	Standard operating systems and firmware supported by provider updates. Applications not auto-patched by a provider quarantined or removed from devices.
Distributed networks	Centralised protection or decentralised strategy set for rental outlets. Audit of connection of "own or non approved devices" to network carried out and risks assessed.
Threat and Health Monitoring	Target Health and Monitoring tools identified. Standard tools built into proprietary software in use identified and "switched on".

Also see section on "Leading Practices examples - Technology"

*Refer to: **Enterprise Security Solutions | Splunk**
Refer to: **Azure Sentinel – Cloud-native SIEM solution | Microsoft Azure

MATURING	LEADER	KPIs
Firewalls established at the boundary between network and internet of all systems and on all devices, where applicable. Blocking policies for all non essential services set.	Penetration testing. Active monitoring and updating of all Firewalls for health and attempted attack status.	"Threat and Health and Monitoring" system KPIs
All in scope systems and devices passworded or code locked with complex passwords. "Dual" or "multi-factor" authentication added for high and medium risk systems.	All in scope systems and devices passworded or code locked with complex passwords. "Dual" or "multi-factor" authentication added for all in scope systems.	"Threat and Health and Monitoring" system KPIs
User level (administrator/operator) accounts established and permissions set. Full user needs review complete and all users on "need to access" basis. Access expiry and renewal controls automated.	Simulated attacks to test access. Active monitoring for health and attempted compromises.	"Threat and Health and Monitoring" system KPIs
User downloads of software applications blocked or restricted to approved sources.	Standardisation of all systems to allow protected network use only. Simulated attacks to test "phishing" and other attacks.	"Threat and Health and Monitoring" system KPIs
Applications and software not actively supported by provider or in-house removed from devices and network servers.	Auto update and refresh process in place for all devices and applications.	Percentage of "up to date" systems in total Inventory
Policies implemented (such as VPN tunnels or equivalent set up for all outlets, if sitting outside central firewalls.) Policy on connection of "own or non approved devices" to network set.	Policy on connection of "own or non approved devices" to network implemented and enforced. Simulated attacks to test access. Active monitoring for health and attempted compromises.	Number/ proportion of unprotected or high/medium risk outlets.
Enterprise-wide tools for health and monitoring implemented. Industry standard system such as "Splunk*" or "Sentinel**" deployed or equivalent in-house suite implemented	Enterprise-wide systems and processes covered by Health and Monitoring and active reporting taking place. Auto alarms and escalation processes supporting process.	Proportion of enterprise-wide systems covered. Number of threats detected and blocked.

PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

ELEMENT	BASE LEVEL
Inventory Management	Inventory of all equipment, systems and software with potential connectivity risk or vulnerability registered and logged.
Policies and Procedures	Formal IT security policies and procedures written and published (internally). All EU and in country legislation identified.
Communications	Policies and procedures communicated formally and in awareness briefings to key staff.
Emergency Response	Outline Emergency Response and crisis management plan established – key players and messages established.
Customer Management	Essential customer requirements (proposals, tenders, reporting, data protection) identified and built into inventory and risk assessment.
Supply Chain Management	OEM and other supply chain vulnerabilities identified and built into inventory and risk assessment.
Maintenance	Asset inventory includes analysis of hardware and software maintenance currently in place and gaps needed to be covered.

Also see section on "Leading Practices examples - Infrastructure"

MATURING	LEADER	KPIs
Inventory refresh process in place. Replacement and redundancy plan for all "end of life", non protectable or insecure elements underway or implemented.	Inventory refresh programme implemented to maintain estate at benchmark cybersecurity levels. All new devices and software added to inventory via formal approval process.	Investment level in inventory refresh programme
Policies and procedures maintained as up to date as required. Policies communicated to all staff actively and shared with strategic customers. Compliance will all legislation.	Cultural acceptance of cybersecurity policies and procedures, driving demonstrated correct behaviours. Policies, procedures and legislation reviewed for update at least annually.	Policies and procedures in place and up to date
Policies and procedures communicated formally and in awareness briefings to key staff. Regular news and updates channel of communications to all staff in place.	Regular news and updates channel of communications to all staff, strategic customers and strategic suppliers in place. "Whistle Blowing" chat or media box in place to allow staff communications up to the security dept.	Number of communications activities and "events"
Emergency Response and crisis management plan implemented for use in emergency and key roles and responsibilities for launch and escalation formalised.	Plan validated and tested by "Attack simulation" and drills at least once a year. Contingency customer communications channels set up.	Successful simulation events. Audit and compliance results.
Engagement with customers to research and identify all important customer risks and priorities for cybersecurity and sharing of information.	Strategic accounts / customers integrated into communications and Health and Threat Monitoring and Continuous Improvement initiatives.	Percentage of strategic customers engaged. Successful tendering results.
Engagement with OEMs and suppliers to communicate down our risks and priorities for cybersecurity and reporting of information.	Strategic suppliers integrated into communications and Health and Threat Monitoring and Continuous Improvement initiatives	Percentage of strategic suppliers engaged.
Standard defence tools, which are built in to proprietary operating systems and software in use, switched on and maintained. Budget committed for ongoing maintenance of securing all high and medium risk systems.	All high and medium risk systems protected by maintained standard or custom built tools and defences with committed ongoing budgets for licence renewals and upgrade paths.	Percentage of IT security budget spent on maintenance versus budget.

A USER CHECKLIST OF THE FOUR FACTOR ELEMENTS TO AID RISK ASSESSMENT AND PRIORITISATION IS ALSO INCLUDED IN THE GUIDE

ERA Cybersecurity — Company Checklist for Intervention Priorities

Capability Element	Maturity level today			Risk Level			Priority for Action
	At or below Base level	At or nearing mid-level maturity	At Leader level	Low	Med	High	1,2,3
PROCESS							
Cybersecurity Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement/Horizon Scanning							
Other?							
PEOPLE							
Entreprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							
Monitoring and Coaching							
Cybersecurity Personnel - Roles and Resp's							
Other?							
TECHNOLOGY							
Inventory Management							
Firewall Management							
Secure configuration							
User access control							
Security update management							
Malware protection							
Distributed Networks							
Threat and Health Monitoring							
Other?							
INFRASTRUCTURE							
Policies and Procedures							
Communications							
Emergency Response							
Customer Management							
Supply Chain Management							
Maintenance							
Other?							

See “Useful templates and tools” on page 104

05

Key Performance Indicators (KPIs)

CYBER INSURANCE

MEASURES AND STANDARDS

What constitutes success for you, what are the KPIs for cybersecurity?

> Rental companies report that cost and cyber ROI over a period are not easily identifiable, so not commonly measured because cybersecurity is an embedded process within all the business processes.

> Most companies measure security costs, but these tend to be aimed at **direct costs** only.

TYPICAL KPIS AND MEASURES OF COST TYPICALLY DEAL WITH DIRECT COSTS AND INCLUDE:

OPERATIONAL MEASURES	RATIOS
Cost of external system, cloud services and software	> Cost per user > Cost per employee > Costs as a percentage of turnover > (adherence to budget, PO' coded purchases, etc.)
Cost of bought-in training	
Cost of external monitoring, SOC, testing	
Cost of insurance	
Cost of an attack or data loss, other incidents	

Operational monitoring of number of attempted attacks, number of data compromise incidents

"6% of IT budget" is considered but not quoted as a common benchmark

Strategic measures

> Avoidance of successful attack
> Cyber maturity
> Digitalisation maturity

HOW IS SUCCESS MEASURED?
Maturity

> **Organisation's chosen maturity framework and risk assessment**

> **Self audit or external audit**

HOW IS SUCCESS MEASURED?
Attack and loss avoidance

> Systems data on attempted and blocked attacks or data compromise events

> Penetration testing...
  > internal,
  > external or,
  > "Bounty - Pay-per-result" process.

Strategic measures

> Avoidance of successful attack

> Cyber maturity

> Digitalisation maturity

A NUMBER OF CYBER KPI, KRI AND ROI CALCULATORS CAN BE USED, BUT NONE REPRESENT LEADING OR ACCEPTED STANDARD METHODS

Technical calculators for ROI and KRI include:

RETURN ON INVESTMENT (ROI) OF CYBERSECURITY

"To calculate a ROI, you must first determine the amount invested. This can vary based on many factors.

Managed Detection & Response (MDR) offerings are less expense and more standardised than **Managed Security Services (MSS)** solutions. Both offer 24×7 protection from cyber threats using a set of tools and expertise."

ROI of Your Cybersecurity Investment - Cipher

KEY RISK INDICATORS AND INDICATORS OF "COMPROMISE"

1. Analysis of key performance indicators (KPIs), key risk indicators (KRIs), and security postures provides a snapshot of how your security team is functioning over time. Helping you better understand what is working and what is worsening, improving decision-making about future projects.
2. Metrics provide quantitative information that you can use to show management and board members you take the protection and integrity of sensitive information and information technology assets seriously.

14 Cybersecurity Metrics + KPIs You Must Track in 2022 | UpGuard

Key measures also include:

> Lost business and customer impact
> Efficiency in identifying a breach
> Analysis by type of attack

38%

Lost business share of total breach costs

Lost business represented the largest share of breach costs, at an average total cost of $1.59M.

287

Average number of days to identify and contain a data breach

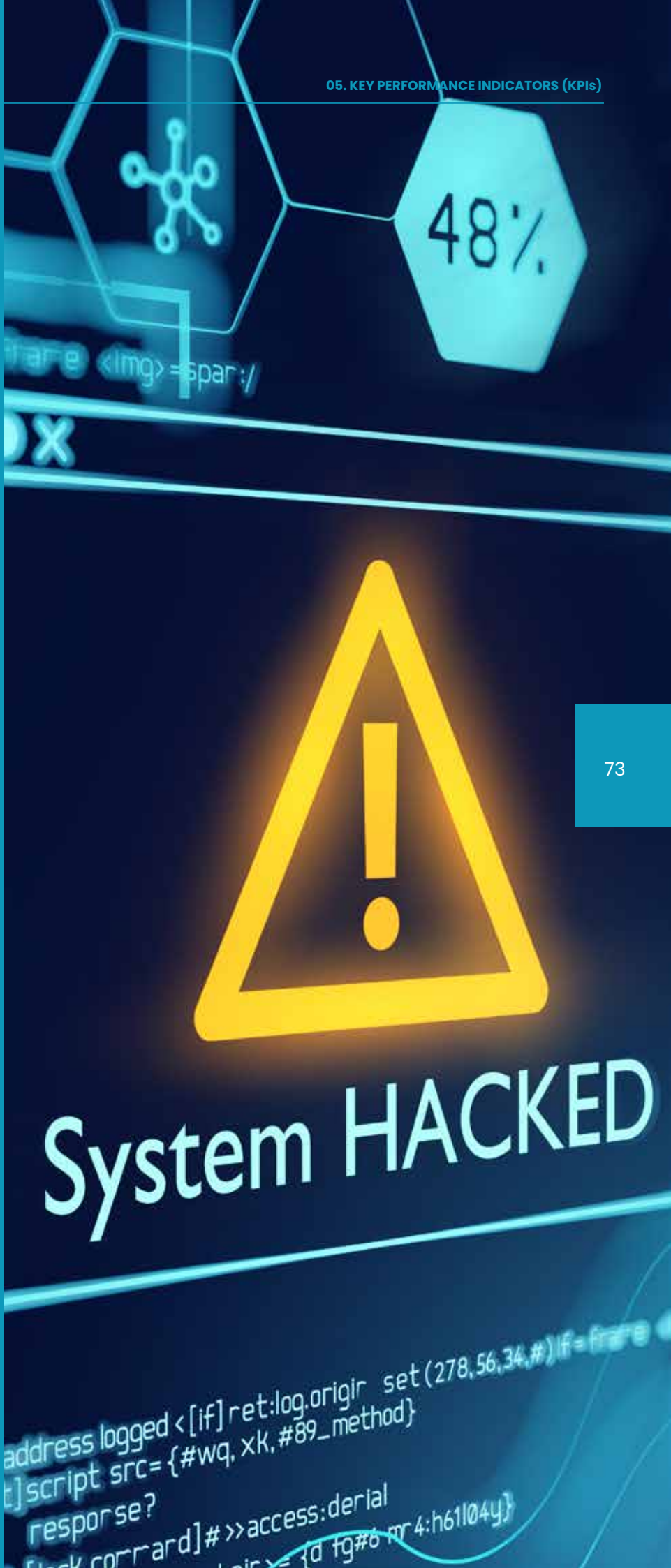
The longer it took to identify and contain, the more costly the breach.

20%

Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

IBM



06

Leading practices illustrated

CYBERSECURITY
LEADING PRACTICES

Leading practices – Process - Inventory and risk assessment are the first steps.

Leaders emphasise that, whilst a comprehensive security plan forms an essential part of a comprehensive strategy, an overarching plan does not have to be the very first step - a full plan may typically come in maturity stages. Leaders stress that it is more important in early stages to take steps to identify all possible high risk areas in the business and prioritise actions to plug or patch vulnerabilities. A comprehensive scan of risks across each of the pillar areas in this guide can be a good starting point. As high risk areas are dealt with, medium risk areas can then be tackled. It is important to say that research indicates that, from a base level, moving up to cover all significant risk areas can be a three to five year process, requiring material and sustained investment.

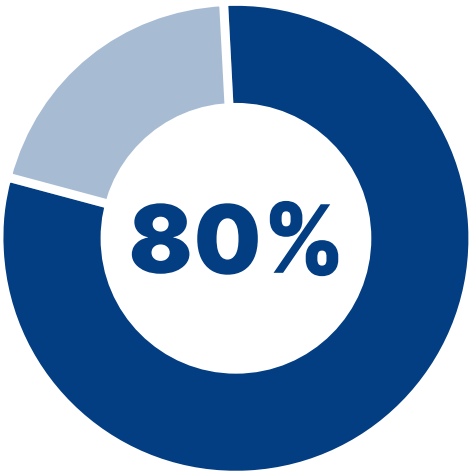
Leader view: strategy driven by risk assessment

Comprehensive and multilayer defence systems require significant investments from the company, which might not be appropriate to the risk involved. Customised systems are best suited for a particular company, individual level plans. Large cyber defence systems at group level attract attention – it's better to have smaller defence systems at local level with limited security layers at central (group) level. Every new project should have its own security measures, on top of a central or horizontal system.

Having decentralised IT systems can in fact decrease vulnerability, as the attacker cannot gain control over the whole system (and multinationals should not have a single, centralised global defence HQ. Individual companies should not have a one-size-fits-all approach, but custom made plans). In the event of a security breach, decentralised systems mean it can be limited to one branch or unit, giving the hacker limited advantage and benefit, allowing time and limiting impact while the breach becomes visible to the whole company and the breach can be "quarantined" and closed down.

So knowing all your assets first, defining points of highest risk, setting a control and response strategy aligned to the risk profiles and then prioritising actions is the key to successful defence.

80% of the problem can be solved by getting the cyber hygiene correct, rather than chasing the latest advanced technology.*



"We don't seek the ultimate in cybersecurity. We do risk assessment based on the assumption that it should be more difficult for a hacker to crack our systems than the systems of other targets, like our competitors."

*Refer to: **29 Must-know Cybersecurity Statistics for 2020 - Cyber Observer (cyber-observer.com)**

Leading Practices - Process - Enterprise-wide accreditation frameworks

Leaders in our industry point to a basic, better, best type of journey to arrive at fit for purpose security, that may use formal accreditations as milestones or be custom built in-house and follow the same principles. A number of international frameworks are in use, two commonly quoted by leaders include:

CYBERSECURITY ESSENTIALS, COMBINED WITH ISO 27001 *

can be a journey from basic, to maturing and on to leader levels of accreditation and compliance in security.

Self-certified UK Government scheme to demonstrate commitment to cybersecurity

Cyber Essentials with hands-on external technical verification from IASME consortium

Often requested in RFPs in some countries

"CIS CONTROLS" **

presents a framework for moving up from basic, to maturing and leader levels of accreditation and compliance in security in a single construct.

ISO27001 is an international standard on how to manage information security

Often requested in RFPs in some countries

International Organization for Standardization

Reference number ISO/IEC 27000:2014(E)

On 24th January 2022 the **NCSC** and IASME implemented an updated set of requirements for Cyber Essentials. This update was the biggest overhaul of the scheme's technical controls since it was launched in 2014 and came in response to the cybersecurity challenges organisations now regularly face.

*Refer to: **About Cyber Essentials - NCSC.GOV.UK**
Refer to: **Cybersecurity Best Practices (cisecurity.org)

> PROCESS

PEOPLE

TECHNOLOGY

INFRASTRUCTURE

CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Leading practices – People – Cybersecurity is not an "IT thing"

There is an important role for Human Resources Management (HR) in cybersecurity defence. Scope of HR intervention and support in leader companies includes:

> **Design and development of policies and procedures** (including GDPR and data protection protocols) and their communication to all staff.

> Adaptation of employee terms and conditions and role descriptions to include **data and security responsibilities**.

> **Enterprise-wide awareness and training on cybersecurity imperatives.**

> **Training needs analysis for front line roles and specific security personnel.** Leaders carry out a mix of in-house training courses and use of external training specialists, particularly where accreditations are being sought.

> **Communications media** such as newsletters or social media bulletins to broadcast latest trends or threats across the enterprise.

> **Set up and hosting of an anonymous "Whistle Blowing" chat or media box** to allow staff to signal potential vulnerabilities that they feel may not be being taken seriously.

> Advanced organisations use techniques such as **"Phishing simulation"** that allows HR to identify retraining or disciplinary needs to address failings in behaviours.

"On the people front, we consider Health and Safety processes as a useful proxy when benchmarking our cybersecurity processes. Electronic safety has many of the same features as physical safety and creating an embedded culture of "Safety in everything we do" is a key message.

People development and training effectiveness need to be audited and measured in the same way as other elements of cybersecurity.

We use "Simulated phishing" - tools to test whether people are recognising and avoiding traps, by testing response to a simulated trap. If errors are made, individual coaching can be targeted with staff; a sustained high error rate by a staff member over time may require a flag with someone's line manager to take corrective action."

"We've had a lot of resistance from people, particularly those in the field, about dual factor authentication. We understood - it made life harder. But it is basics and just had to be done."

"Computers, networks and software don't create cyber risks and vulnerabilities. The people who design them, implement them and operate them do. Awareness, roles and responsibilities and training are some of the most powerful and accessible tools everyone has at their disposal to prevent and manage weaknesses."

Leading practices – People - Cybersecurity is a "People thing"

TRAIN IN THE ESSENTIALS AND GENERATE AWARENESS FIRST. LOW COST, HIGH IMPACT.

Working to get all the basics covered doesn't have to cost a lot. Communications and awareness briefing, policy setting, training on activation of protection tools in standard products, firewalls, software vulnerability patching, why user permissions are needed and what "need only access" means - these are all things that can be educated in, without great cost and planning delay.

EMBED CYBERSECURITY INTO THE ORGANISATION AND ALL ROLES, ENTERPRISE-WIDE.

Organisationally, all leaders stress that cybersecurity is an enterprise-wide responsibility and not just part of an IT function. Most companies will aim to have at operational level one (and in larger companies perhaps two) personnel in Information Security Officer roles. Whilst these roles, by their nature, belong to the Information Technology function and typically report into this function, IT Directors stress their responsibilities are broad - and extend right across the organisation.

MEASURE AND TEST PEOPLE'S COMPLIANCE, UNDERSTANDING AND EFFECTIVENESS.

People development and training effectiveness need to be tested, audited and measured in the same way as other elements of cybersecurity.

Increasing maturity

> "Where we have lower skilled or technology averse employees, we adapt to fit human limitations. Paradoxically, using paper can be a valid part of cyber protection. Whilst moving processes online and deploying technology and automation is undoubtedly the way things will be, by exception, if we find that it is too difficult for some staff, particularly those in blue collar basic functions in depot or distributed activities to operate a function or send data via online access, reluctantly - we will leave it on paper. Where that is best for cyber safety, that takes precedence."

Low skilled or remote location staff may need low technology solutions to support cybersecurity needs

> A lot of people think you can put in technology layer on layer to protect you, but actually simpler and low cost interventions in how you manage people and behaviours can have more impact, especially in the early stages.

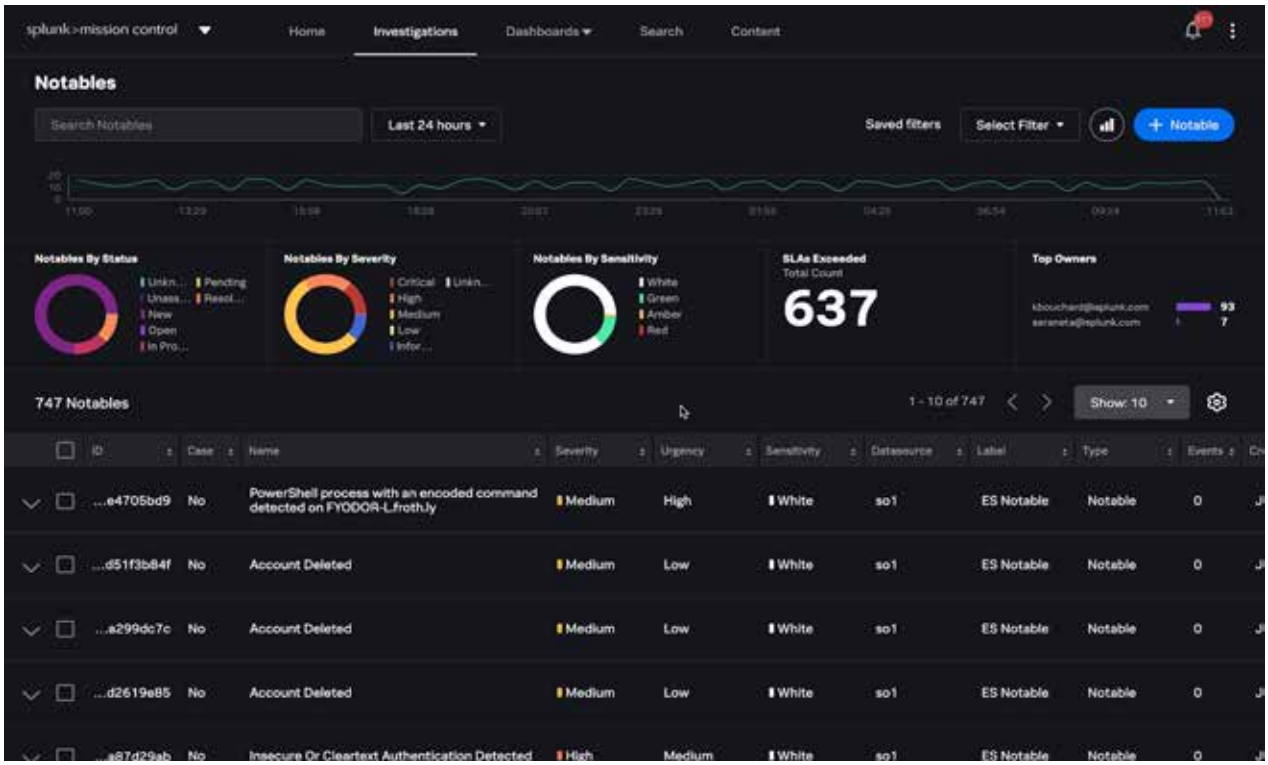
Information Technology tools continue to develop rapidly and provide a powerful means of cyber defence, for "early warning" and threat interception.

LEADING PRACTICES EXAMPLE
THREAT AND HEALTH MONITORING – SET UP OF A "SOC"

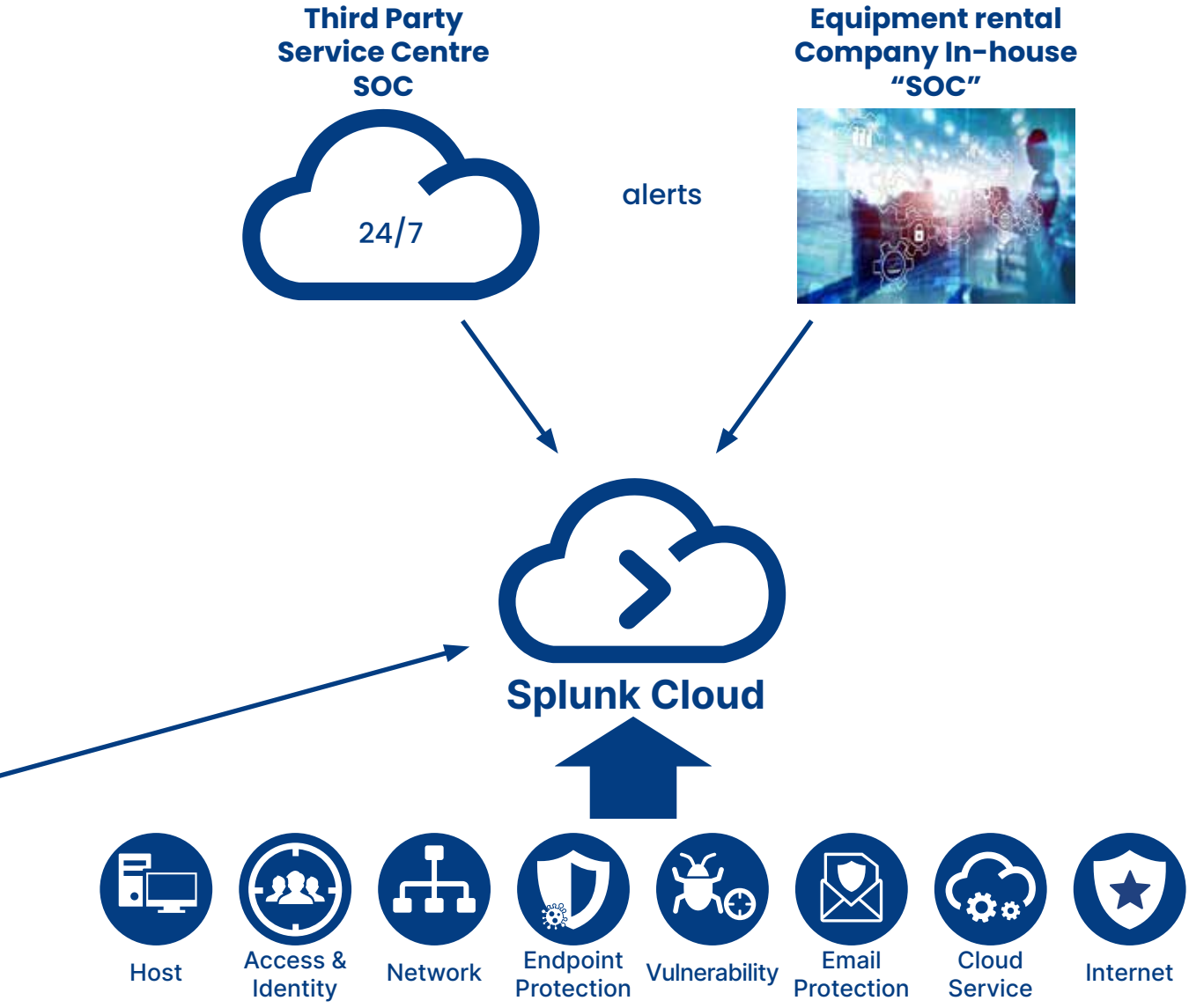
Establishing a **"SOC" (Security Operations Centre)** is essential to get the most out of the power of automated systems.

Leaders may operate an in-house SOC, often supplemented by third party centres which can offer 24×7 support cover and advanced monitoring and management services. A shared centre service provided by a third party is also considered a good way for less advanced or smaller organisations to get access to high quality Health and Threat Monitoring, when an in-house one may not be justifiable.

Equipment rental company example: "Splunk"* *- Splunk and integrated third party and in-house "SOC" in use, identifying and signalling threats real time across the enterprise*



*Refer to: **Enterprise Security Solutions | Splunk**



> The combined SOC runs on a single Splunk* platform.

> Updated and actively monitored 24×7×365.

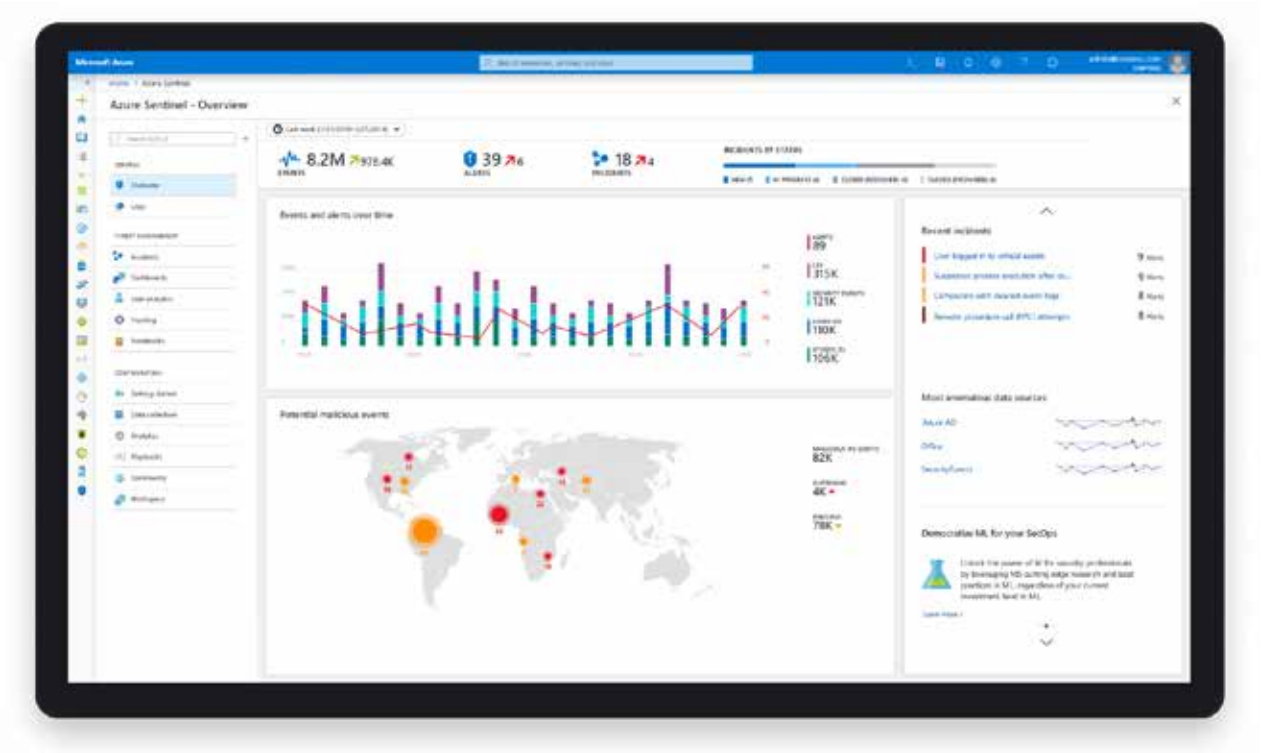
> **Security Service Provider SOC** - support, troubleshooting, development, health monitoring, incident response.

> **In-house SOC** – "hourlies" refresh and review, hunts for malicious behaviour, investigates tickets raised by SOC and users.

Threat and health monitoring – Enterprise-wide diagnostics

Most of the leading monitoring and alarm systems are considered effective and valuable tools in the fight against attack. Those most commonly quoted by leaders in equipment rental as in active use are “Microsoft Azure Sentinel”* and “Splunk”*.

“MS Azure Sentinel”* identifying and signalling threats across the enterprise



TECHNOLOGY CAN HELP TO AUDIT THE EFFECTIVENESS OF CYBERSECURITY USER EXAMPLE**

Quarterly audits to simulate attacks and report on company performance can include:

> **“OSINT” for Digital Asset Discovery** - “Open Source Intelligence” identifies the public attack surface of the company.

> **Security Assessment (Blackbox)** – Automated audit routines from outside the company, with no inside knowledge.

> **Security Assessment (Whitebox)** – Audit routines using accounts set up with different permission groups.

*Refer to: **Azure Sentinel – Cloud-native SIEM solution | Microsoft Azure**
Enterprise Security Solutions | Splunk

Refer to: **Open-source intelligence - Wikipedia

> Use of available technology and automation for Health and Threats is crucial... But remember, there is no point investing in the technologies, if you do not also place infrastructure around it to be able to respond on a "24 x 7" basis. Hackers don't work office hours, so what happens if the system alarms sound at midnight?

THE SOC AND ITS REPORTING INFORMS GOVERNANCE OF IT SECURITY

Governance may be set at two levels through process and committee structures; first, overall strategy and governance can be through an Executive Committee, with representatives from operational delivery, HR, Finance and Legal as well as IT; second, project level governance is focused around approval committees that ensures all projects (not just system and IT projects) considers cybersecurity implications and builds in essential safeguards. New developments and systems projects are required to seek launch approval at architecture stage, showing how cybersecurity essentials will be "designed in" from "Ground zero".

Advanced users also link the systems to real time intelligence globally from leading bodies. Those commonly in use amongst leaders include the following:

> Data feeds can be added to systems real time to maintain a full inventory of latest threats. Many sources exist and can be added in. Some of those in use in our sector include:

- AlienVault OTX - Malware, Malicious actor IP source. **https://otx.alienvault.com/api**
- SANS Internet Storm Centre - Top malicious IP from global honey pots. **https://isc.sans.edu/tools/**
- Malware Domains - Domains used by malware. **CIS Center for Internet Security (cisecurity.org)**
- National Cybersecurity Centre – CISP.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

ALIEN VAULT

INTERNET STORM CENTER

Leaders also recommend membership of leading international bodies, sharing information and data on cybersecurity

CiSP approved member

CiSP - NCSC.GOV.UK

enisa

Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)

National Cyber Security Centre
a part of GCHQ

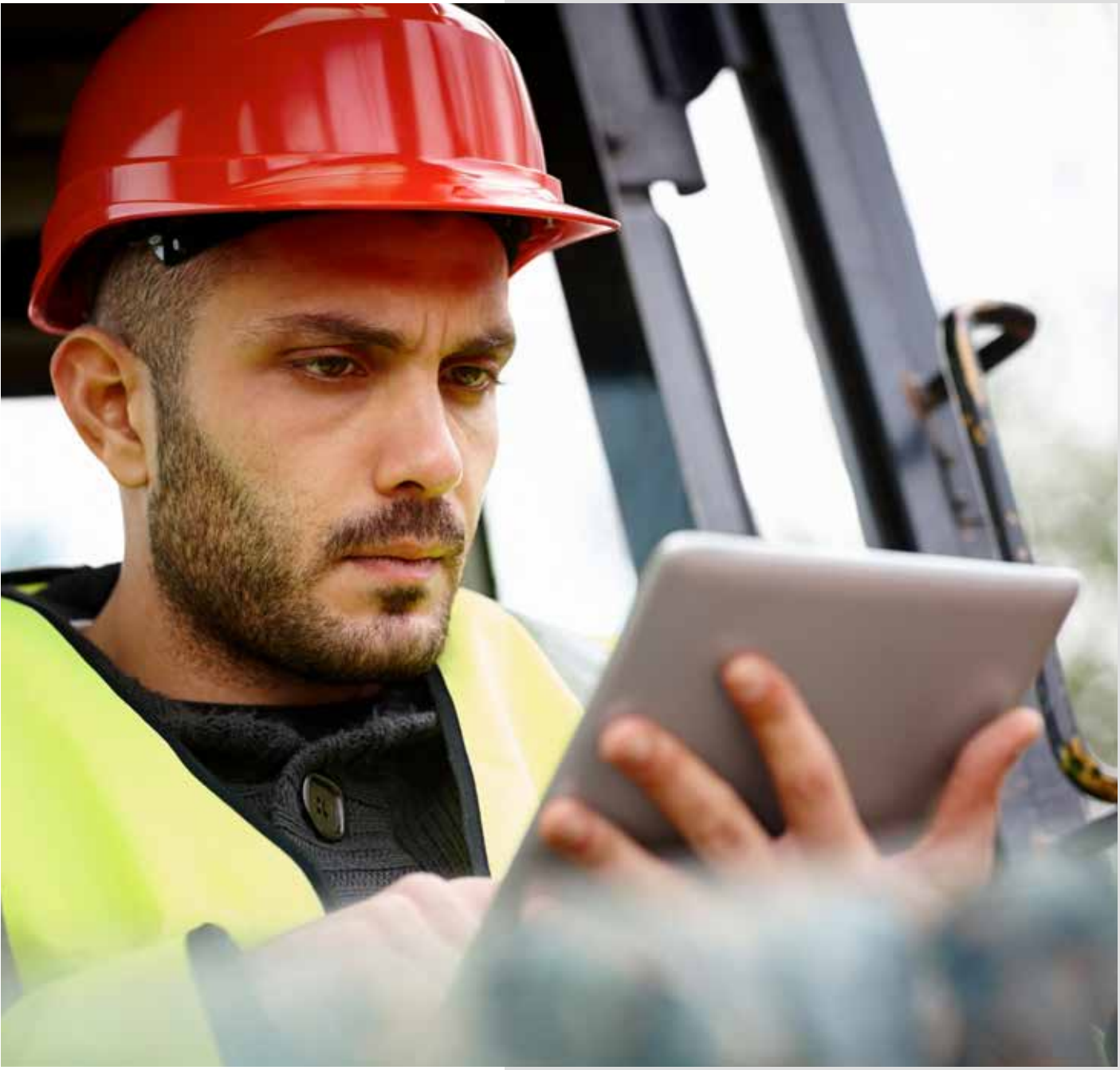
National cybersecurity Centre - NCSC.GOV.UK

PROCESS

PEOPLE

> TECHNOLOGY

INFRASTRUCTURE



CYBER VULNERABILITY

TECHNOLOGY IS BEING EXPLOITED TO DECEIVE

Human behaviour and weaknesses are fair game

DEEPFAKE VOICE

The CEO of a large energy corporation transferred **€220,000 to a Hungarian supplier.** The CEO believed he was talking to his boss and acted swiftly to transfer the funds as directed. Only he wasn't talking to his boss. Hackers successfully impersonated his boss's voice, and the CEO believed it to be him. Most people think that they could tell the difference between someone's real voice and an impersonation, but voice skins sound precisely like the individual being impersonated.

To mimic someone's voice, recordings of that person's voice must exist, and you'd be surprised at how often someone in your organisation is recorded. Webinars, YouTube videos, speeches, Ted talks, company training sessions, even smart speakers.

What is Deepfake and Why Is It a Major Cybersecurity Risk? **Hitachi Systems Security - Your Cybersecurity Experts (hitachi-systems-security.com)**

DEEPFAKE VIDEO

At the most basic level, deepfakes can be used to trick the facial recognition software that many consumers and businesses rely on for access control. This makes deepfakes among the top threats to cloud security.

Gearing Up Security for the Deepfake Era - Blog | GlobalSign

> Cyber investment is not just about threat avoidance, having trained people and having formal qualifications has opened up new rental markets for us that are typically more regulated, like Defence and Government sectors.

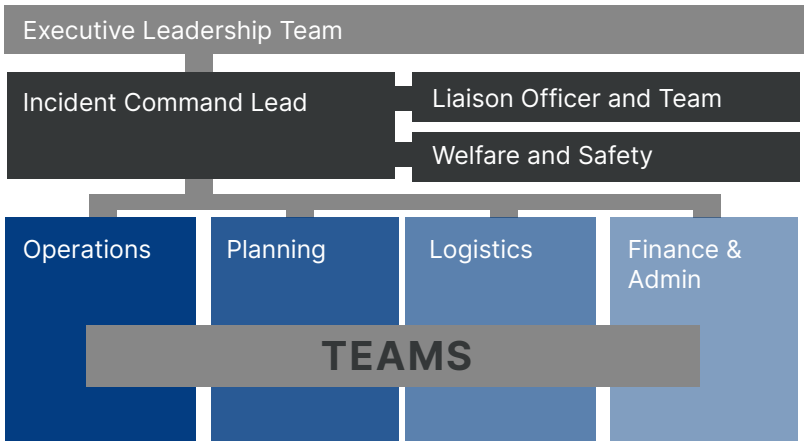
Response to cyber attack

PREPARATIONS IN THE EVENT OF AN ATTACK

"If the worst happens, despite all the best prevention measures, you have to be ready with an **Incident Management Plan.**"

Leader example - Crisis Management Planning

> Adopt Incident Command System (ICS) for Crisis Management



- > Establish a framework
- > Launch the crisis management process
- > Emergency Approval Process
- > Establish clear guidelines for escalation
- > Appoint communications lead
- > Develop a communications portion of existing incident response plan
- > Map the stakeholders (customers, media, partners, regulators, employees, vendors)
- > Develop draft media statements
- > Host a table-top exercise
- > Designate a Cyber Lead from Legal
- > Review policies and public statements
- > Conduct Cybersecurity Assessments and Tests (include direction from Legal Department)
- > Conduct regular board briefings
- > Manage third party vendors

PROCESS

PEOPLE

TECHNOLOGY

> INFRASTRUCTURE

TRIAGE AND COMMUNICATIONS

"The First 48 Hours"

If the worst happens, despite all the best prevention measures, leaders stress two things in the first period after an attack...

> First ... "**Don't react too much or too soon. Make a calculated assessment and define an appropriate response**".

Attacks can come in many forms but one of the most serious types can be a **"Ransomware attack"**. In a systems denial situation, an immediate emergency response is needed but a process needs to have been put in place to assess and "Triage" the situation:

- Does this incident merit classification as an emergency?
- Is it ongoing? Should emergency response plans be activated now?
- Who can authorise disconnection from the network, the internet and closedown of a system that writes business?
- When will that permission to act be empowered?
- When will that escalation to higher levels of intervention (that may impact ability to do business) be triggered and who are the authorised decision makers?
- Who should be informed first and when?

Is the attack financially or politically motivated?

Snapshot of reported attacks in a single month of 2022! ...

July 2022. Hackers targeted Iran's Islamic Culture and Communication Organization (ICCO). The attack took down at least 6 websites, placed images of Iranian resistance leaders on 15 additional sites, wiped databases and computers, and allowed hackers to obtain access to sensitive ICCO data.
July 2022. A hacker claimed to acquire records on 1 billion Chinese from a Shanghai police database and posted the data for sale online.
July 2022. Belgium's Foreign Ministry accused China of a cyber espionage campaign against Belgian targets, including Belgium's Ministries of Interior and Defence. A Chinese Embassy in Belgium spokesperson denied the accusations.
July 2022. Hackers targeted social media accounts owned by the British Royal Army. The attack included the takeover of the British Army's Twitter and YouTube accounts.
July 2022. Hackers temporarily took down websites belonging to the Albanian Prime Minister's Office and the Parliament, and the e-Albania portal used to access public services.
July 2022. Hackers breached a Ukrainian media company to broadcast on multiple radio stations that Ukrainian President Volodymyr Zelenskyy was in critical condition. Zelenskyy refuted the claims and blamed Russia for the attack.
July 2022. China stated the United States stole 97 billion pieces of global internet data and 124 billion pieces of telephone data in June, specifically blaming the National Security Agency (NSA)'s Office of Tailored Access Operations (TAO).

“Often, even with advanced monitoring and technology, it is not clear what is happening or what has happened and whether it is continuing. You have to stop and ask yourself... “What is really happening now, how serious is it? Should I step in and start shutting things down immediately that will impact our business?

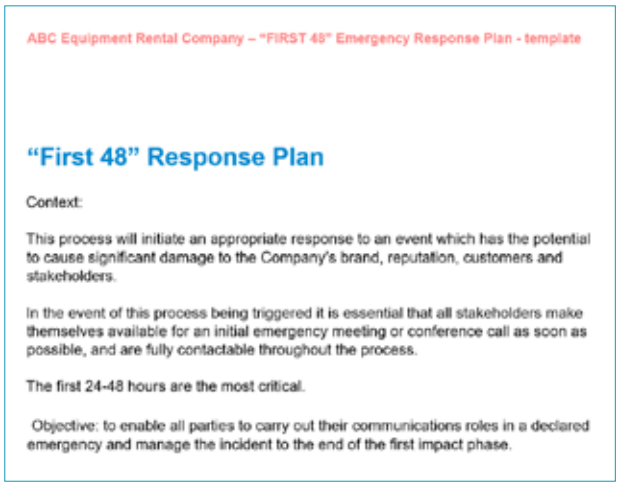
You can do more harm than the threat itself by responding too quickly, or in a panic, to stop a breach or a data loss.”

If the worst happens, despite all the best prevention measures, leaders stress two things in the first period after an attack...

> Second **... Communicate, communicate, communicate**

Leaders believe that it is crucial to have a **"First 48 hours response plan"** to manage communications to staff, customers, suppliers and stakeholders.

The plan may form part of the company's overall disaster response and business continuity plan and stand as a cybersecurity Incident Management Plan.



ABC Equipment Rental Company – "FIRST 48" Emergency Response Plan - template

"First 48" Response Plan

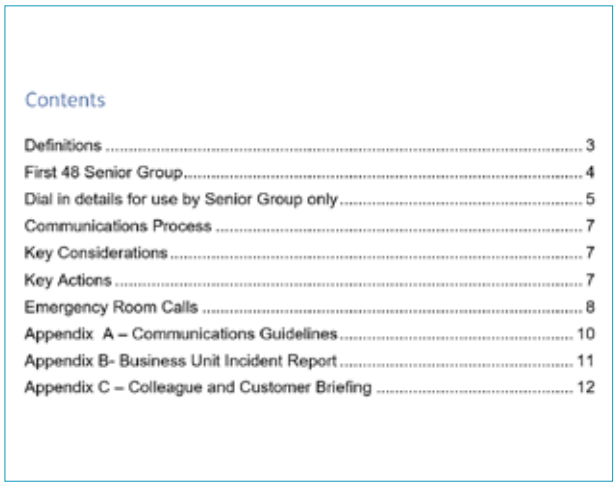
Context:

This process will initiate an appropriate response to an event which has the potential to cause significant damage to the Company's brand, reputation, customers and stakeholders.

In the event of this process being triggered it is essential that all stakeholders make themselves available for an initial emergency meeting or conference call as soon as possible, and are fully contactable throughout the process.

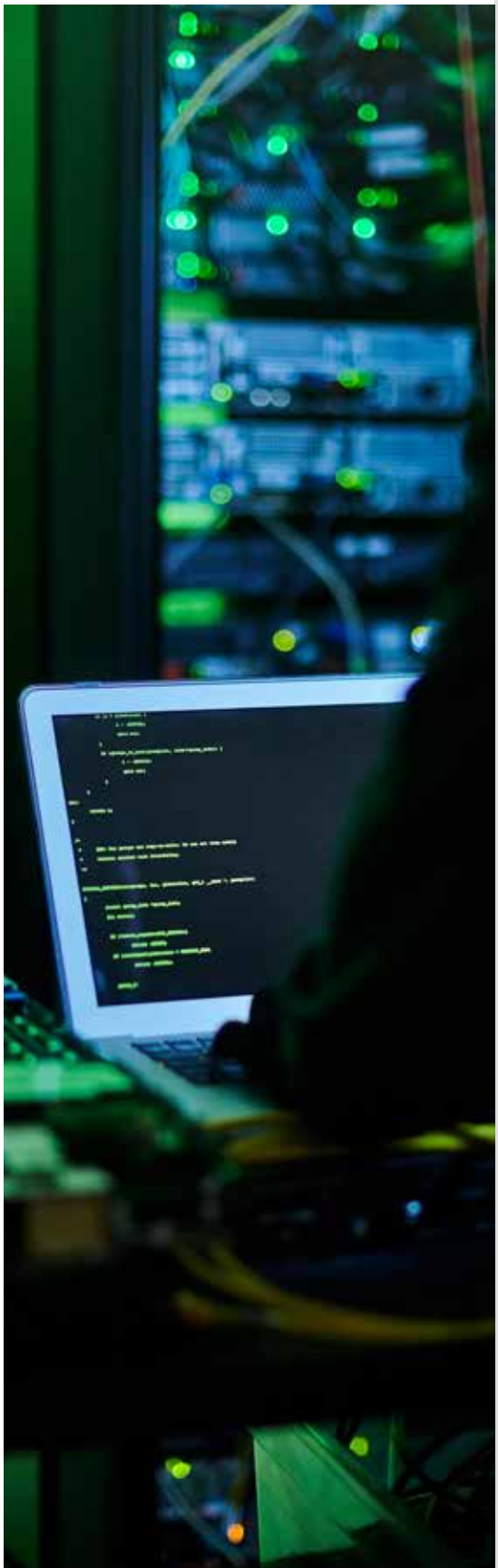
The first 24-48 hours are the most critical.

Objective: to enable all parties to carry out their communications roles in a declared emergency and manage the incident to the end of the first impact phase.



Contents

A step-by-step "First 48" template has been adapted from model examples, offered by leader companies and is included at the end of this guide for user reference and further adaptation to their own circumstances. See page 104 for usable templates.



> An attack is just like a real war in many ways. In the "Fog of War" you don't know if something is really wrong. Assessment and clarity of understanding is key at the start of the onslaught.
>
> The decision to escalate to the 2 or 3 people at most in your organisation, who have the power to say *"Stop everything"* is a pivotal moment.

CYBERSECURITY
IN CONCLUSION

Prepare for a secure future

THE RACE FOR GOOD IT SECURITY WILL NEVER END, BUT TO STAY AHEAD, EQUIPMENT RENTAL COMPANIES MUST:

1. Know their assets, strengths and vulnerabilities.
2. Carry out risk assessment.
3. Plan and invest appropriately.
4. Prepare, in case the worst happens.
5. Refresh and continuously improve.

“The “Internet of Things” (IoT*) will never cease to bring new challenges and threats ...

Security is the biggest concern in adopting “Internet of Things” technology, with concerns that rapid development is happening without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary.

Most of the technical security concerns are similar to those of conventional servers, workstations and smartphones. These concerns include using weak authentication, forgetting to change default credentials, unencrypted messages sent between devices, **SQL injections**, **Man-in-the-middle attacks**, and poor handling of security updates. However, many IoT devices have severe operational limitations on the computational power available to them. These constraints often make them unable to directly use basic security measures such as implementing firewalls or using strong cryptosystems to encrypt their communications with other devices - and the low price and consumer focus of many devices makes a robust security patching system uncommon.

*Refer to: **Internet of things - Wikipedia**

Internet of Things devices also have access to new areas of data, and can often control physical devices, so that even by 2014 it was possible to say that many Internet-connected appliances could already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats.[1] Computer-controlled devices in automobiles such as brakes, engines, locks, hood and trunk releases, horns, heating, and dashboards have been shown to be vulnerable to attackers who have access to the on-board network. In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely.

CYBER STRATEGY

THE NEXT 3 YEARS FOR "LEADERS"?

No revolution but massively more maturity and digital enablement

WHAT WILL DRIVE CYBERSECURITY STRATEGY INVESTMENT IN THE NEXT THREE YEARS?

1. Advancing up the maturity curve.

> **No revolution** - "Leaders" are modest about their situation and consider they are not high enough up on the maturity scale.

> Although ERA Cybersecurity WG members are modest about their levels of maturity many are clearly advanced in many cyber aspects - but their focus remains on reinforcement, discipline and hardening of existing strategies and processes.

> No member appeared motivated to move strategy to leading edge or sunrise technologies such as Cyber AI, but several pointed to more demanding testing and penetration systems (such as "bounty pay per result systems") which will inform and confirm maturity levels and drive further hardening of defences, develop better KPIs.

2. Develop cyber defence capability to support *outward* facing Digital enablement.

> Above all, members point to the drive towards digital enablement across the business, which means more and extended "open" platforms.

> They do not think this will create new vulnerabilities, but stress that early stage digitalisation has been data warehousing and internal process focused. The future thrust is increasingly on "end to end" data and platform integration with customers, equipment and other suppliers, where alignment and common cyber lines of defence end to end will be the key challenge.

For those members in markets geographically close to the Ukrainian conflict, there has been an increased push to develop cyber defences

The data imperative may see customers seeking to *bypass the rental company altogether* and communicate directly with data warehouse sources and with smart equipment

"Digitalisation is increasing our automation, reducing the number of people in process activity so dramatically reducing scope for human error and so cyber /data risk."

Useful templates and tools

USEFUL TEMPLATES AND TOOLS

User versions of:

1. ENTERPRISE-WIDE CYBERSECURITY: RISK ASSESSMENT CHECKLIST - TEMPLATE

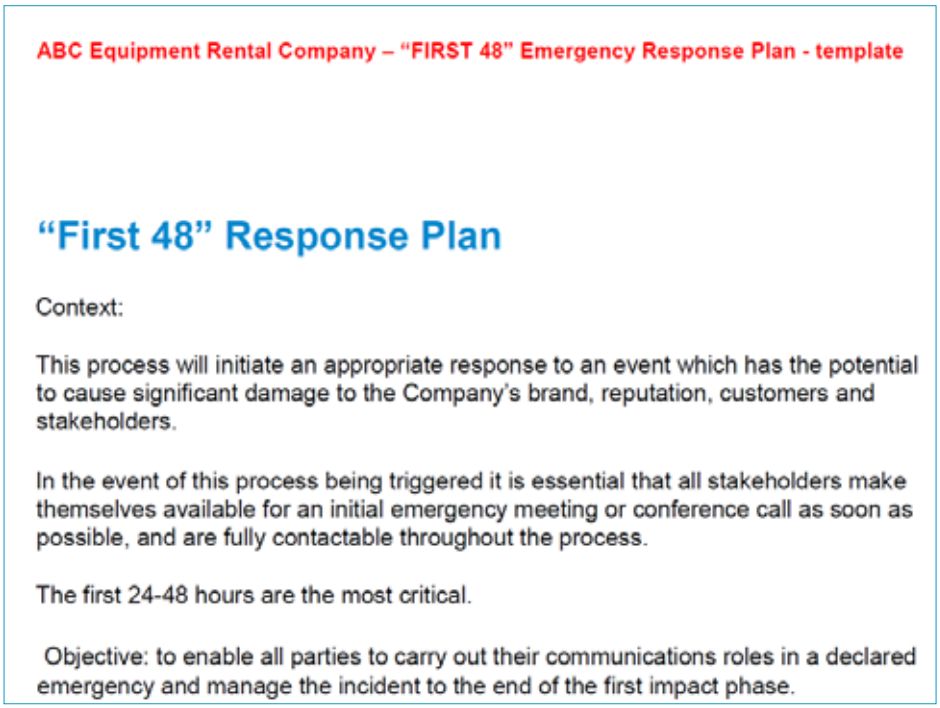
Please see the according Word (.doc)

ERA Cybersecurity — Company Checklist for Intervention Priorities

Capability Element	Maturity level today			Risk Level			Priority for Action
	At or below Base level	At or nearing mid-level maturity	At Leader level	Low	Med	High	1,2,3
PROCESS							
Cybersecurity Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement/Horizon Scanning							
Other?							
PEOPLE							
Entreprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							
Monitoring and Coaching							
Cybersecurity Personnel - Roles and Resp's							
Other?							
TECHNOLOGY							
Inventory Management							
Firewall Management							
Secure configuration							
User access control							
Security update management							
Malware protection							
Distributed Networks							
Threat and Health Monitoring							
Other?							
INFRASTRUCTURE							
Policies and Procedures							
Communications							
Emergency Response							
Customer Management							
Supply Chain Management							
Maintenance							
Other?							

2. EMERGENCY RESPONSE: "FIRST 48" PLAN – TEMPLATE

Please see the according Word (.docx)



ABC Equipment Rental Company – "FIRST 48" Emergency Response Plan - template

"First 48" Response Plan

Context:

This process will initiate an appropriate response to an event which has the potential to cause significant damage to the Company's brand, reputation, customers and stakeholders.

In the event of this process being triggered it is essential that all stakeholders make themselves available for an initial emergency meeting or conference call as soon as possible, and are fully contactable throughout the process.

The first 24-48 hours are the most critical.

Objective: to enable all parties to carry out their communications roles in a declared emergency and manage the incident to the end of the first impact phase.

ABC Equipment Rental Company – "FIRST 48" Emergency Response Plan - template

Contents

ACKNOWLEDGEMENTS

The guide has been compiled with the invaluable support and contributions of ERA member companies, led by:

REFERENCES

References used in this guide include the following:

CONTEXT	ORIGIN	REFERENCE
Worldwide cybersecurity statistics	Cybersecurity Ventures	Cybersecurity Ventures - Spending 2021 – 2025
		Cybersecurity Ventures - Global Ransomware Damage Costs Predictions
	Cybersecurityintelligence.com	Cybercrime To Cost The World $10.5 Trillion Annually By 2025
		Corporate Cyber Attacks Up 50%
	Verizon	Verizon
	IBM	IBM
	Gartner	Gartner – Survey
	Hiscox UK	The Hiscox Cyber Readiness Report 2022 | Hiscox UK
	Cyber-Observer.com	29 Must-know Cybersecurity Statistics for 2020 - Cyber Observer (cyber-observer.com)
European cybersecurity Legislation	EU NIS directive	NIS Directive | Shaping Europe's digital future (europa.eu)
		NIS2 Directive
GPS Tracker Vulnerabilities (MiCODUS MV720)	BitSight	Critical vulnerabilities in widely used vehicle gps tracker
Cyber Attacks	For Construction Pros	Tech Tips: Telematics | For Construction Pros
	Construction Europe	How to keep smart construction machines safe from hackers
EU Machinery Regulation	International Rental News	EU Machinery Regulation to impact rental
	Europa.eu	Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
Cybersecurity Budget Spending	ENISA (references Gartner)	NIS Investments 2021 (ENISA report)
Cybersecurity best practices	National cybersecurity Centre, UK	About Cyber Essentials - NCSC.GOV.UK
	Center for Internet Security	Cybersecurity Best Practices (cisecurity.org)

CONTEXT	ORIGIN	REFERENCE
Threat and health monitoring	Microsoft.com	Azure Sentinel – Cloud-native SIEM solution | Microsoft Azure
	Splunk.com	Enterprise Security Solutions | Splunk
	AT&T Alien Labs	OTX DirectConnect API - AlienVault - Open Threat Exchange
	Sans Internet Storm Center	InfoSec Tools - SANS Internet Storm Center
	Center for Internet Security	CIS Center for Internet Security (cisecurity.org)
Cyber Security Information and Data Sharing	National Cyber Security Centre	CISP - Cyber Security Information Sharing Partnership - NCSC.GOV.UK
		National Cyber Security Centre - NCSC.GOV.UK
	European Union Agency for Cybersecurity	Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)
Cyber KPI, KRI and ROI	Cipher	Managed Detection & Response (MDR)
		Managed Security Services (MSS)
		ROI of Your Cybersecurity Investment – Cipher
	Upguard	14 Cybersecurity Metrics + KPIs You Must Track in 2022 | UpGuard
Cyber Vulnerability	Wall Street Journal	Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case – WSJ
	Hitachi System Security	Hitachi Systems Security - Your Cybersecurity Experts (hitachi-systems-security.com)
	GlobalSign	Cloud Security: Top 3 Threats (globalsign.com)
"OSINT" for Digital Asset Discovery - "Open Source Intelligence	Wikipedia	Open-source intelligence - Wikipedia
The "Internet of Things" (IoT)	Wikipedia	Internet of things – Wikipedia
		SQL injection – Wikipedia
		Man-in-the-middle attack - Wikipedia