ERA guide to cybersecurity leading practice in the equipment rental industry

Are you equipped for the challenge?

ERA guide to cybersecurity – Purpose of this guide

One of the greatest threats to our industry is the vulnerability to cybersecurity impacts on our businesses.

In 2021, there is no established roadmap in 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 this guide 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, research with rental companies suggests there is limited specific direction for our sector. This guide aims to offer 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 renta HSS Hire
RIWAL Boels RENTAL KILOUTOU CGT A TESYA COMPANY

Guide contents

Guide contents

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.

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”. 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.

Worldwide spending on cybersecurity is going to reach $133.7 billion in 2022. (Gartner)

The damage related to cybercrime is projected to hit $6 trillion annually in 2021, according to Cybersecurity Ventures

In 2020, 71% of breaches were financially motivated and 25% were motivated by espionage. 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively. (Verizon).

All equipment rental companies use some, or all, of these channels and systems as “Digitialisation” gathers pace, so everyone, *regardless of size and maturity in our industry,* is at risk.

Our industry now needs an ongoing community amongst European companies to collaborate on cybersecurity best practice, common threats and issues facing us all.

Views of equipment rental Leaders…

> You may think you can stay under the radar, but the on line 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 *specia*l 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.

- 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 has been 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.

Views of equipment rental Leaders…

“

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 threats – *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 response may require evidence to the customer that an equipment rental company operates a nationally or internationally recognised cybersecurity framework (see page 25 for examples) 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 appoint is flagged as a major risk for entry by an attacker into a organisations network “through the back door” and then on 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.

Views of equipment rental Leaders..

“

As a younger (five years 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?”

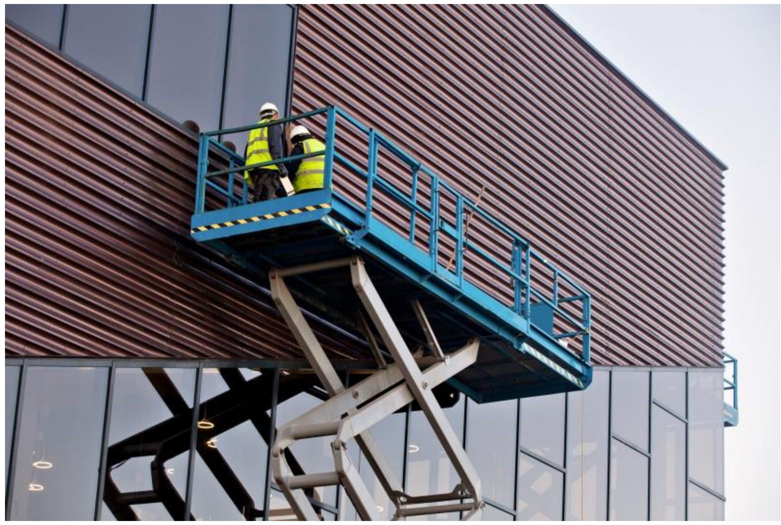
”

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.

Concerns are 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.



Views of equipment rental Leaders…

"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."

Views of equipment rental Leaders…

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 OEM's 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.

Cybersecurity threats – equipment rental companies face all the same challenges as other sectors …. but we also have *special factors* …

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 operation 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 (HSM's) needs to be substantial and may not always be justifiable in business terms but essential for cybersecurity.

Views of equipment rental Leaders…

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" with 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 strategy.

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

Views of equipment rental Leaders…

> You have to protect data transmission and networks 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.

Cybersecurity in our industry is also increasingly a legislative and regulatory matter

EU legislation is centered 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.

NIS Directive | Shaping Europe's digital future (europa.eu)

The (the NIS Directive) provides 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 scope of the NIS Directive continues to increase. Latest changes under consideration may …

- Extend the coverage of essential sectors and establishes a list of important sectors.
- Lay down cybersecurity risk management and reporting obligations for companies in essential and important sectors.
- Introduce European cybersecurity certification schemes.

*Refer to: *Directive on security of network and information systems*

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.

Guide contents

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.

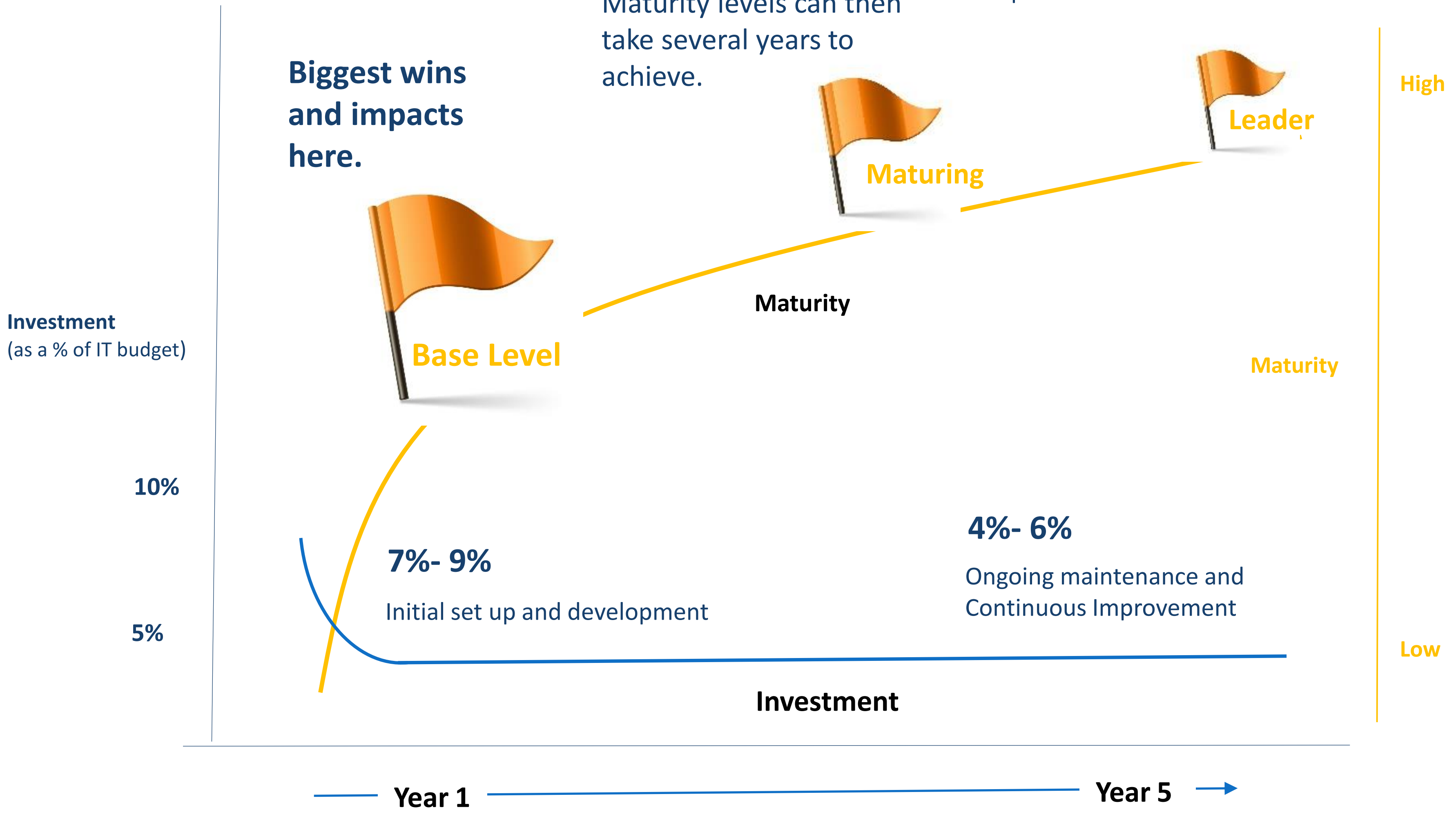
But above all, the biggest progress and wins can come quickly at the start by low cost measures to get the basics in place…..

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.

Leadership means “fit for purpose” not scaling the ultimate peak.

Maturity levels can then take several years to achieve.

Biggest wins and impacts here.



7%- 9%

Initial set up and development

4%- 6%

Ongoing maintenance and Continuous Improvement

Views of equipment rental Leaders…

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.

Cybersecurity in equipment rental companies – investment and maturity

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 (50 percent)**: 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 percent)**: 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) (16 percent)**: 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 percent)**: 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."

Global views:

The cost of vulnerability

Cybersecurity budgeting has been increasing steadily as more decision-makers are realizing the value and importance of cybersecurity investments. According to the cybersecurity mid-year snapshot'19 report, Cybersecurity budgets have increased by almost 60%.

- *By the end of 2020, security services are expected to account for 50% of cybersecurity budgets. (Gartner)*
- *The average cost of a malware attack on a company is $2.6 million. (Accenture)*
- *$3.9 million is the average cost of a data breach. (IBM)*
- *The average cost in time of a malware attack is 50 days. (Accenture)*
- *The most expensive component of a cyber-attack is information loss at $5.9 million. (Accenture)*
- *Including turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill, the cost of lost business globally was highest for U.S. companies at $4.13 million per company. (Ponemon Institute)*
- *50% of large enterprises (with over 10,000 employees) are spending $1 million or more annually on security, with 43% spending $250,000*

The most common causes of data breach reported in 2020**:

- *Weak and Stolen Credentials (Passwords)*
- *Back Doors, Application Vulnerabilities*
- *Malware*
- *Social Engineering*
- *Too Many Permissions*
- *Insider Threats*
- *Improper Configuration and User Error*

*Refer to: IT Key Metrics Data 2019: Key IT Security Measures: by Industry (gartner.com)

**Refer to: https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/

Guide contents

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.

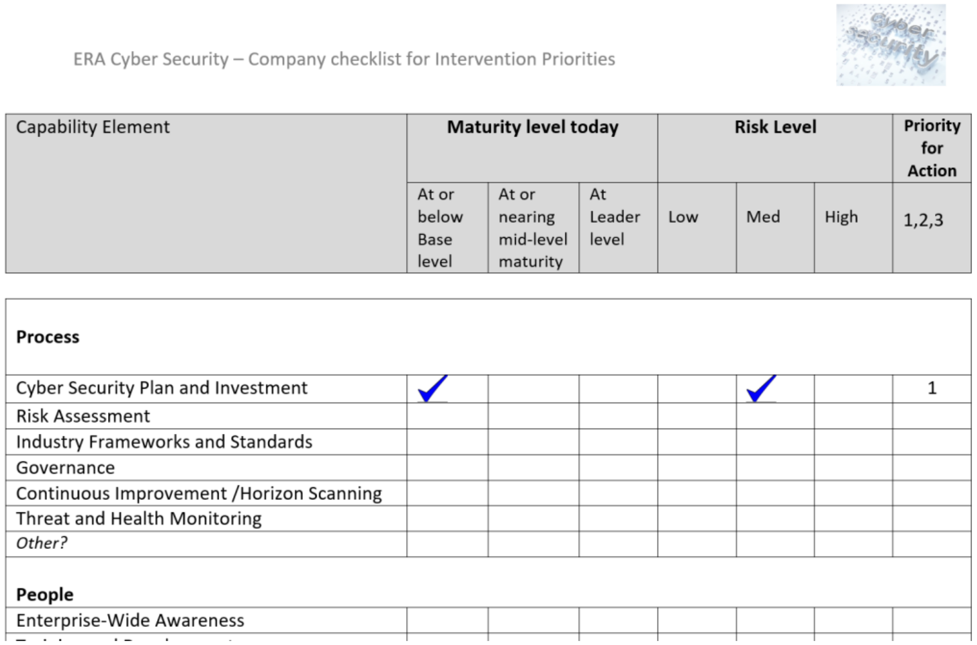
Leaders emphasise that, whilst a comprehensive security plan forms an essential part of an overall business strategy, "an over-arching plan" does not have to be the very first step - a full plan may typically come in maturity stages. It is most important in early stages to take steps to identify all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

"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) (KPI's) in place. The roadmap in this guide also indicates typical measures and performance measurement systems in use today by leader companies.

A checklist for scope, risk assessment and prioritisation based on the four elements in the roadmap is included as a useful template (see page 36).



ERA Cyber Security – 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							
Cyber Security Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement /Horizon Scanning							
Threat and Health Monitoring							
Other?							
People							
Enterprise-Wide Awareness							

Enterprise-wide cybersecurity – Scope of intervention for equipment rental companies

The focus for cybersecurity intervention is often around technology and systems, however many risks have root cause in human behaviour, robustness of processes and monitoring, reporting and response 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

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

Customers

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

Process ✓

People

Technology

Infrastructure

Features of each maturity level:

Element	Base Level	Maturing	Leader	KPI's
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.	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 Assessment	High, medium and low risks identified enterprise-wide. Action plans for highest priorities set.	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
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.	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	Key governance issues and reporting processes identified. Strategic players to form governance group in organisation identified.	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.
Continuous Improvement and Horizon Scanning	Awareness of latest threats and anticipated future trends, to feed into base level planning	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.

Also see section on **"Leading practices examples – Process"**

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

Cybersecurity in equipment rental companies – Maturity Stages

Process
People ✓
Technology
Infrastructure

Features of each maturity level:

Element	Base Level	Maturing	Leader	KPI's
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.	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 and Development	Relevant first and second line populations, requiring training identified and training needs set.	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.
Roles and Responsibilities	First and second line staff roles and responsibilities, within day to day security context, identified and added to core role descriptions.	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 defence, added to their roles.
Monitoring and Coaching	Using high priority risk assessment, all staff in high risk areas or failing base level training, given individual coaching and "retesting"	Penetration testing and "Phishing" simulations to test competencies for first line staff.	Penetration testing and "Phishing" simulations to test competencies for all staff.	No of incidents or successful attacks with human error factor.
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	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 manhours to cybersecurity as a proportion of overall staff resources and IT hours/costs.

Also see section on **"Leading practices examples – People"**

Cybersecurity in equipment rental companies – Maturity Stages

Process

People

Technology ✓

Infrastructure

Features of each maturity level:

Element	Base Level	Maturing	Leader	KPI’s
Firewall Management	Firewalls established at the boundary between network and internet of all high and medium risk systems and devices.	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 KPI’s
Secure configuration	All high and medium risk systems passworded or code locked - default passwords changed. Non essential programmes and software deleted.	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 KPI’s
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.	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 KPI’s
Malware protection	Anti-malware software installed on high and medium risk systems and devices. Malware warning alarms activated.	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 KPI’s
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.	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
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.	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.
Threat and Health Monitoring	Target Health and Monitoring tools identified. Standard tools built into proprietary software in use identified and “switched on” .	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.

Also see section on **“Leading Practices examples - Technology”**

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

Cybersecurity in equipment rental companies – Maturity Stages

Process

People

Technology

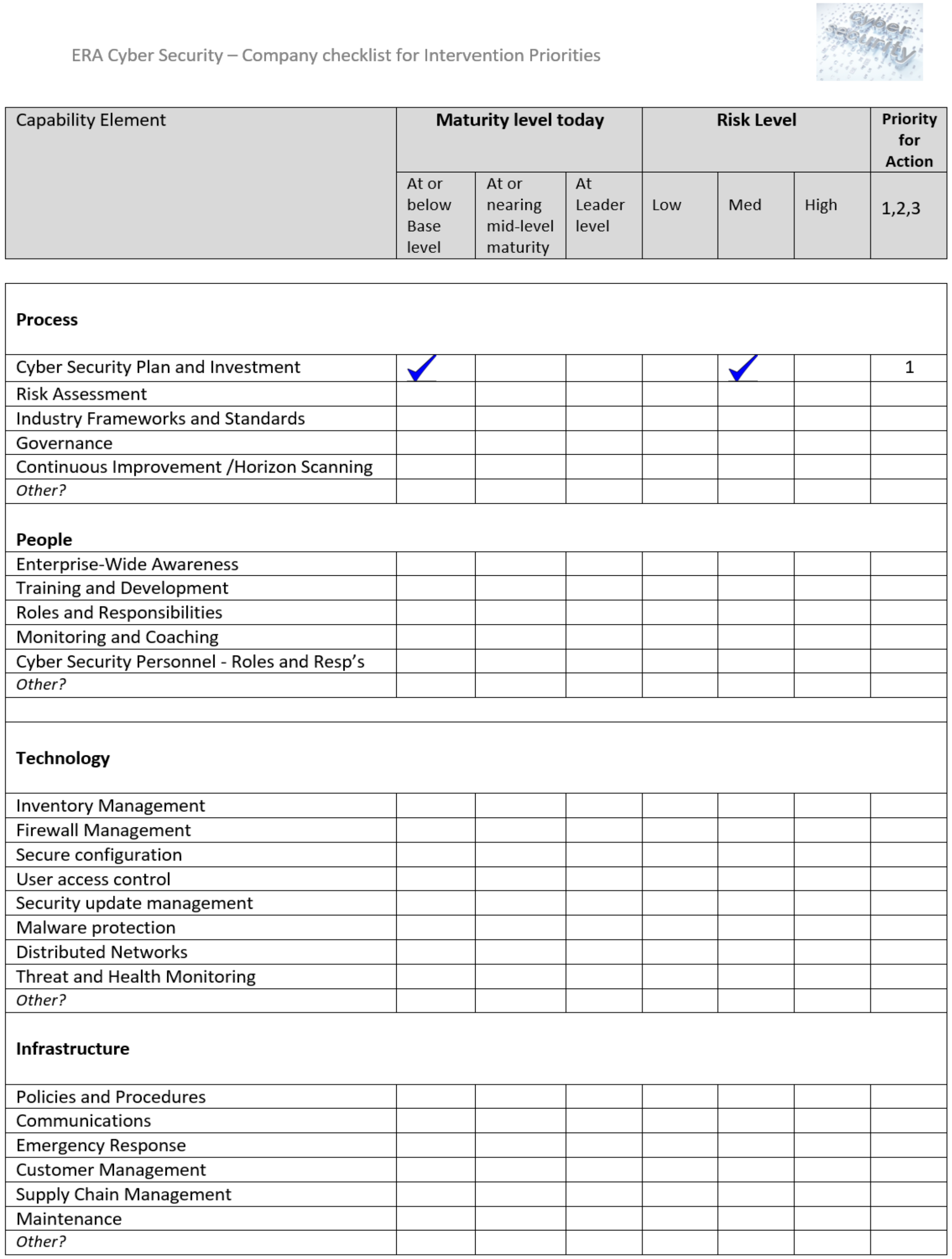
Infrastructure ✓

Features of each maturity level:

Element	Base Level	Maturing	Leader	KPI's
Inventory Management	Inventory of all equipment, systems and software with potential connectivity risk or vulnerability registered and logged.	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	Formal IT Security policies and procedures written and published (internally). All EU and in country legislation identified.	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 legislative reviewed for update at least annually.	Policies and procedures in place and up to date
Communications	Policies and procedures communicated formally and in awareness briefings to key staff.	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	Outline Emergency Response and crisis management plan established – key players and messages established.	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.
Customer Management	Essential customer requirements (proposals, tenders, reporting, data protection) identified and built into inventory and risk assessment.	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.
Supply Chain Management	OEM and other supply chain vulnerabilities identified and built into inventory and risk assessment.	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.
Maintenance	Asset inventory includes analysis of hardware and software maintenance currently in place and gaps needed to be covered.	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.

Also see section on **"Leading Practices examples – Infrastructure"**

A user checklist of the four factor elements to aid risk assessment and prioritisation is also included in the guide



ERA Cyber Security – 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							
Cyber Security Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement /Horizon Scanning							
Other?							
People							
Enterprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							
Monitoring and Coaching							
Cyber Security 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 36

Guide contents

Cybersecurity – Leading practices

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

Process ✓

People

Technology

Infrastructure

Leaders emphasise that, whilst a comprehensive security plan forms an essential part of a comprehensive strategy, an over arching 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. Customized 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).

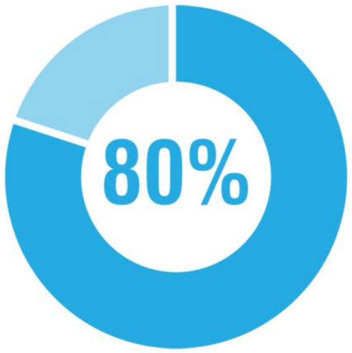
In the event of a security breach, decentralised systems mean it can be limited to one branch or unit, giving the hacker limited advantage and benefit, allowing time and limiting impact while the breach becomes visible to the whole company and the breach can be "quarantined" and closed down.

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.

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

Views of equipment rental Leaders…

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.



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

Cybersecurity – Leading practices

Leading Practices - Process - Enterprise-wide accreditation frameworks

Process ✓

People

Technology

Infrastructure

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.

CYBER ESSENTIALS

Self-certified UK Government scheme to demonstrate commitment to cybersecurity

CYBER ESSENTIALS PLUS

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

Often requested in RFPs in some countries

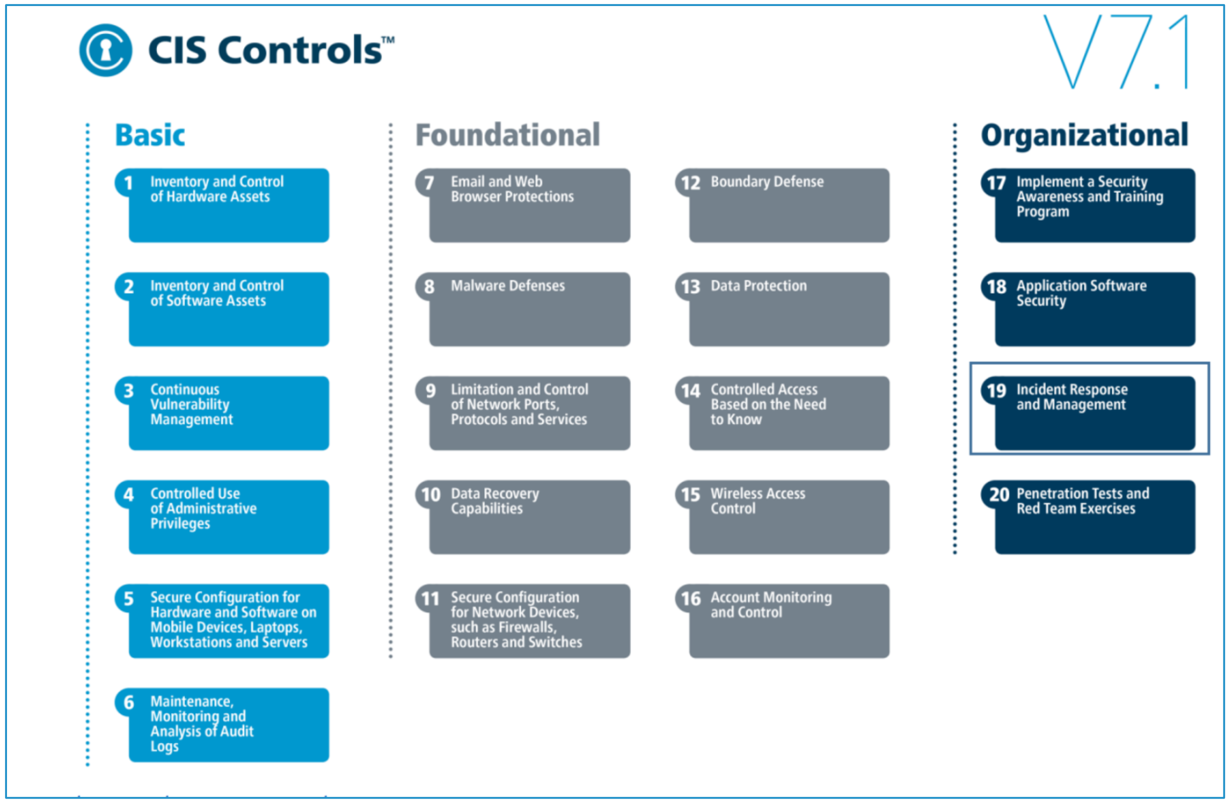
Information Security Management System ISO 27001 Certified

ISO27001 is an international standard on how to manage information security

Often requested in RFPs in some countries

ISO International Organization for Standardization IEC Reference number ISO/IEC 27000:2014(E)

"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.



CIS Controls™ V7.1

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

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

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

Cybersecurity – Leading practices

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

Process

People ✓

Technology

Infrastructure

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.

Views of equipment rental Leaders…

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.

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.

Cybersecurity – Leading practices

Leading practices – People - Cybersecurity is a “People thing”

Process

People ✓

Technology

Infrastructure

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

Views of equipment rental Leaders…

> 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.

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

> 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 on line 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.

Cybersecurity – Leading practices

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

Process

People

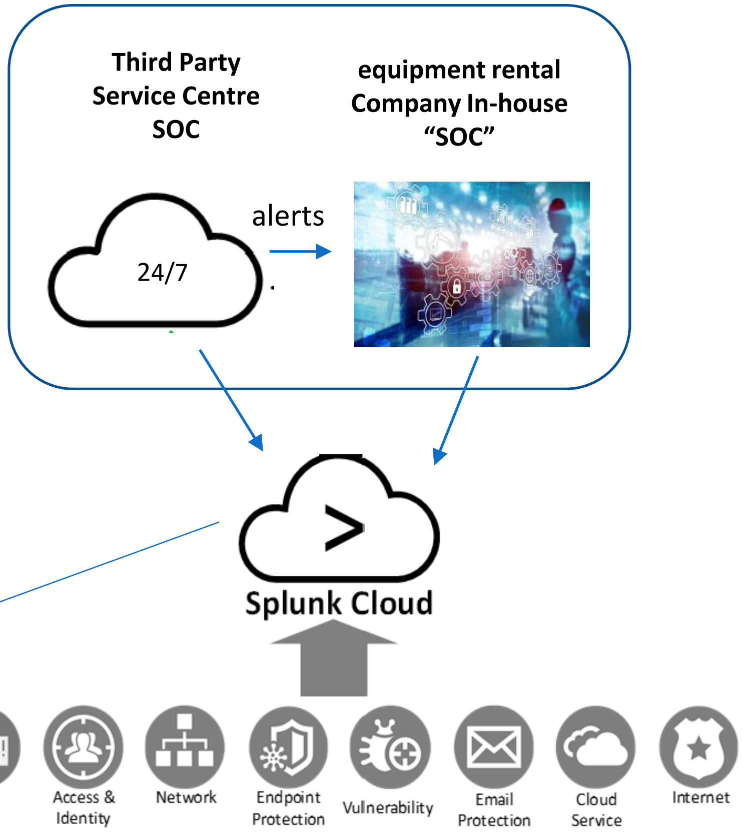
Technology ✓

Infrastructure

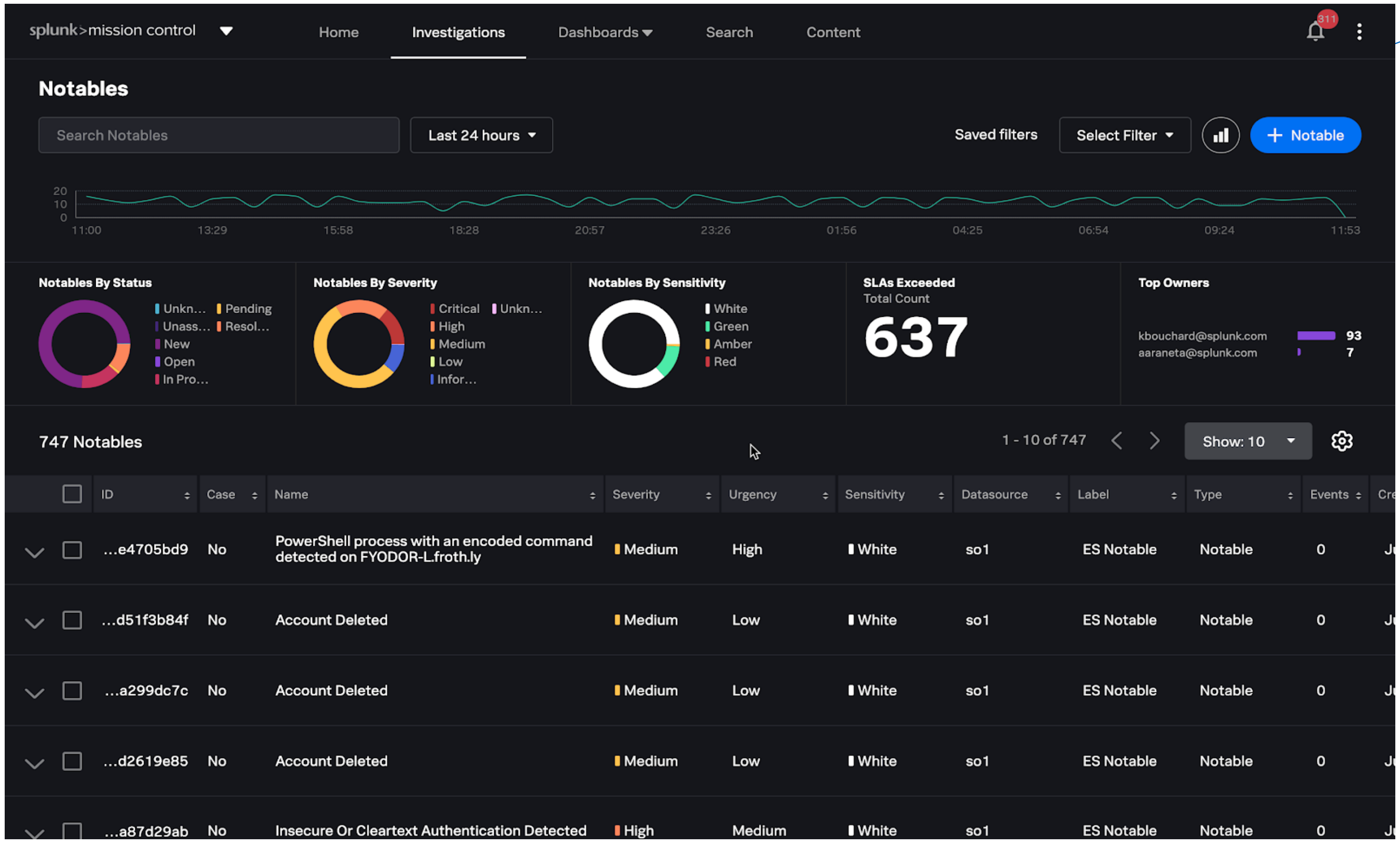
Leading practices example – Threat and Health Monitoring – set up of a "SOC"

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 24x7 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*



Notables

Search Notables | Last 24 hours | Saved filters | Select Filter | + Notable

Notables By Status

Notables By Severity

Notables By Sensitivity

SLAs Exceeded
Total Count
637

Top Owners

kbouchard@splunk.com	93
aaraneta@splunk.com	7

747 Notables

1 - 10 of 747 | Show: 10

	ID	Case	Name	Severity	Urgency	Sensitivity	Datasource	Label	Type	Events	Cre
□	…e4705bd9	No	PowerShell process with an encoded command detected on FYODOR-L.froth.ly	Medium	High	White	so1	ES Notable	Notable	0	J
□	…d51f3b84f	No	Account Deleted	Medium	Low	White	so1	ES Notable	Notable	0	J
□	…a299dc7c	No	Account Deleted	Medium	Low	White	so1	ES Notable	Notable	0	J
□	…d2619e85	No	Account Deleted	Medium	Low	White	so1	ES Notable	Notable	0	J
□	…a87d29ab	No	Insecure Or Cleartext Authentication Detected	High	Medium	White	so1	ES Notable	Notable	0	J

- The combined SOC runs on a single Splunk* platform.
- Updated and actively monitored 24x7x365.
- **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.

*Refer to: Enterprise Security Solutions | Splunk

Cybersecurity – Leading practices

Threat and health monitoring – Enterprise-wide diagnostics

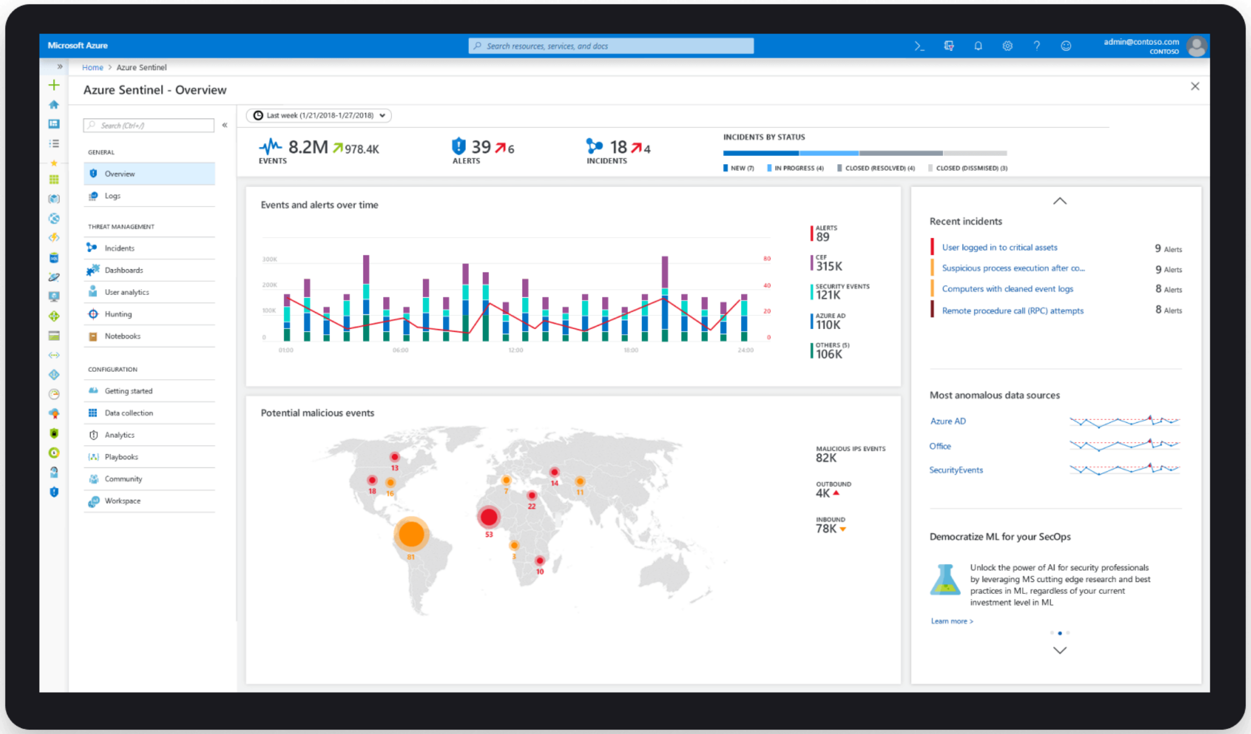
Process

People

Technology ✓

Infrastructure

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*".



*Refer to: [Azure Sentinel – Cloud-native SIEM solution | Microsoft Azure](#)
[Enterprise Security Solutions | Splunk](#)

"MS Azure Sentinel"* identifying and signalling threats across the enterprise

Views of equipment rental Leaders…

"

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?

"

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:

[Open-source intelligence - Wikipedia](#)

Cybersecurity – Leading practices

Health and threat Monitoring – Enterprise-wide diagnostics

Process

People

Technology ✓

Infrastructure

The SOC and its reporting informs governance of IT Security

Governance may be set at two levels through process and committee structures; firstly overall strategy and governance can be through and Executive Committee, with representatives from operational delivery, HR, Finance and Legal as well as IT; secondly 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:

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

- 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.

ALIEN VAULT

INTERNET STORM CENTER

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

CiSP | approved member
Cyber-security Information Sharing Partnership

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

National Cyber
Security Centre

CiSP - NCSC.GOV.UK

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

National cybersecurity Centre - NCSC.GOV.UK

Cybersecurity – Leading practices

Response to Cyber attack – Preparations in the event of an attack

Process

People

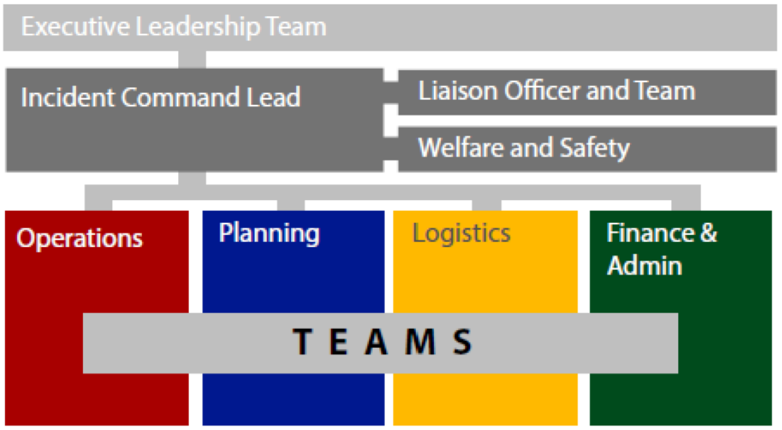
Technology

Infrastructure ✓

> "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

Cybersecurity – Leading practices

Response to Cyber attack – Triage and communications – "The First 48 Hours"

Process

People

Technology

Infrastructure ✓

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

- **Firstly … "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?

Views of equipment rental Leaders.

> 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.

Is the attack financially or politically motivated?

March 2021. The head of U.S. Cyber Command testified that the organization had conducted more than two dozen operations to confront foreign threats ahead of the 2020 U.S. elections, including eleven forward hunt operations in nine different countries.
March 2021. A group of Chinese hackers used Facebook to send malicious links to Uyghur activists, journalists, and dissidents located abroad.
March 2021. The Indian Computer Emergency Response Team found evidence of Chinese hackers conducting a cyber espionage campaign against the Indian transportation sector
March 2021. Polish security services announced that suspected Russian hackers briefly took over the websites of Poland's National Atomic Energy Agency and Health Ministry to spread false alerts of a nonexistent radioactive threat.
March 2021. Both Russian and Chinese intelligence services targeted the European Medicines Agency in 2020 in unrelated campaigns, stealing documents relating to COVID-19 vaccines and medicines.
March 2021. Ukraine's State Security Service announced it had prevented a large-scale attack by Russian FSB hackers attempting to gain access to classified government data.
March 2021. Lithuania's State Security Department declared that Russian hackers had targeted top Lithuanian officials in 2020 and used the country's IT infrastructure to carry out attacks against organizations involved in developing a COVID-19 vaccine.
March 2021. Suspected Iranian hackers targeted government agencies, academia, and the tourism industry in Azerbaijan, Bahrain, Israel, Saudi Arabia, and the UAE as part of a cyber espionage campaign.
March 2021. Chinese government hackers targeted Microsoft's enterprise email software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.
March 2021. Suspected Chinese hackers targeted electricity grid operators in India in an apparent attempt to lay the groundwork for possible future attacks.

Response to an attack – Triage and Communications – "The First 48 Hours"

Process

People

Technology

Infrastructure ✓

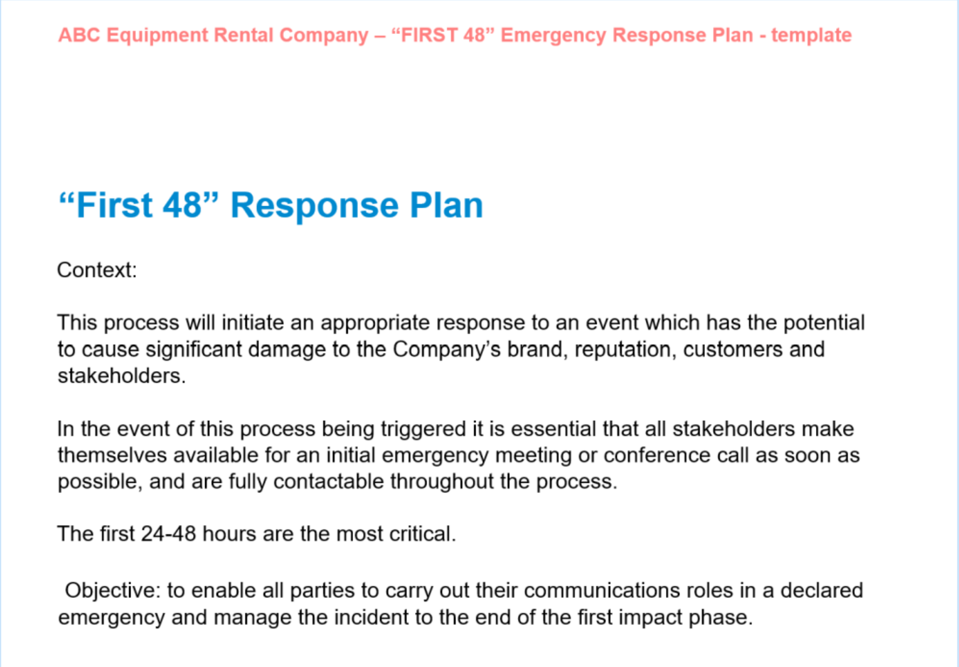
If the worst happens, despite all the best prevention measures, Leaders stress two things in the first period after an attack….

- **Secondly …. 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.

A step-by-step "First 48" template has been adapted from model examples, offered by leader companies and is included at the of this guide for user reference and further adaptation to their own circumstances. See page 36 for usable templates.



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

"First 48" Response Plan

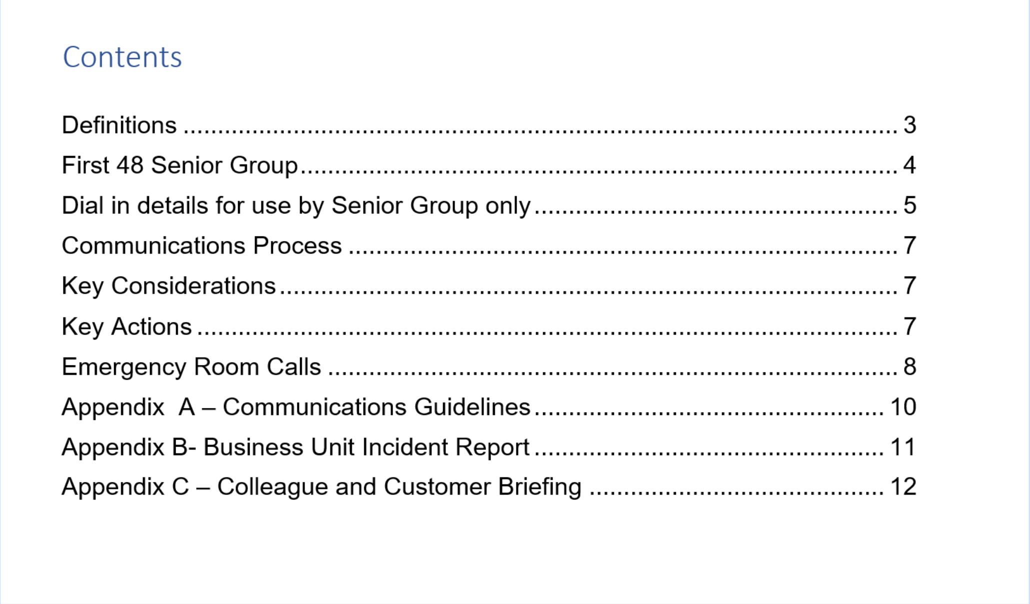
Context:

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

Views of equipment rental Leaders…

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.

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.[Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard 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.

*Refer to: Internet of things - Wikipedia

Guide contents

Useful templates and tools

User versions of:

1. Enterprise-wide cybersecurity: Risk assessment checklist - template
2. Emergency Response: "First 48" plan - template

Useful Templates and Tools

ERA Cyber Security – Company checklist for Intervention Priorities

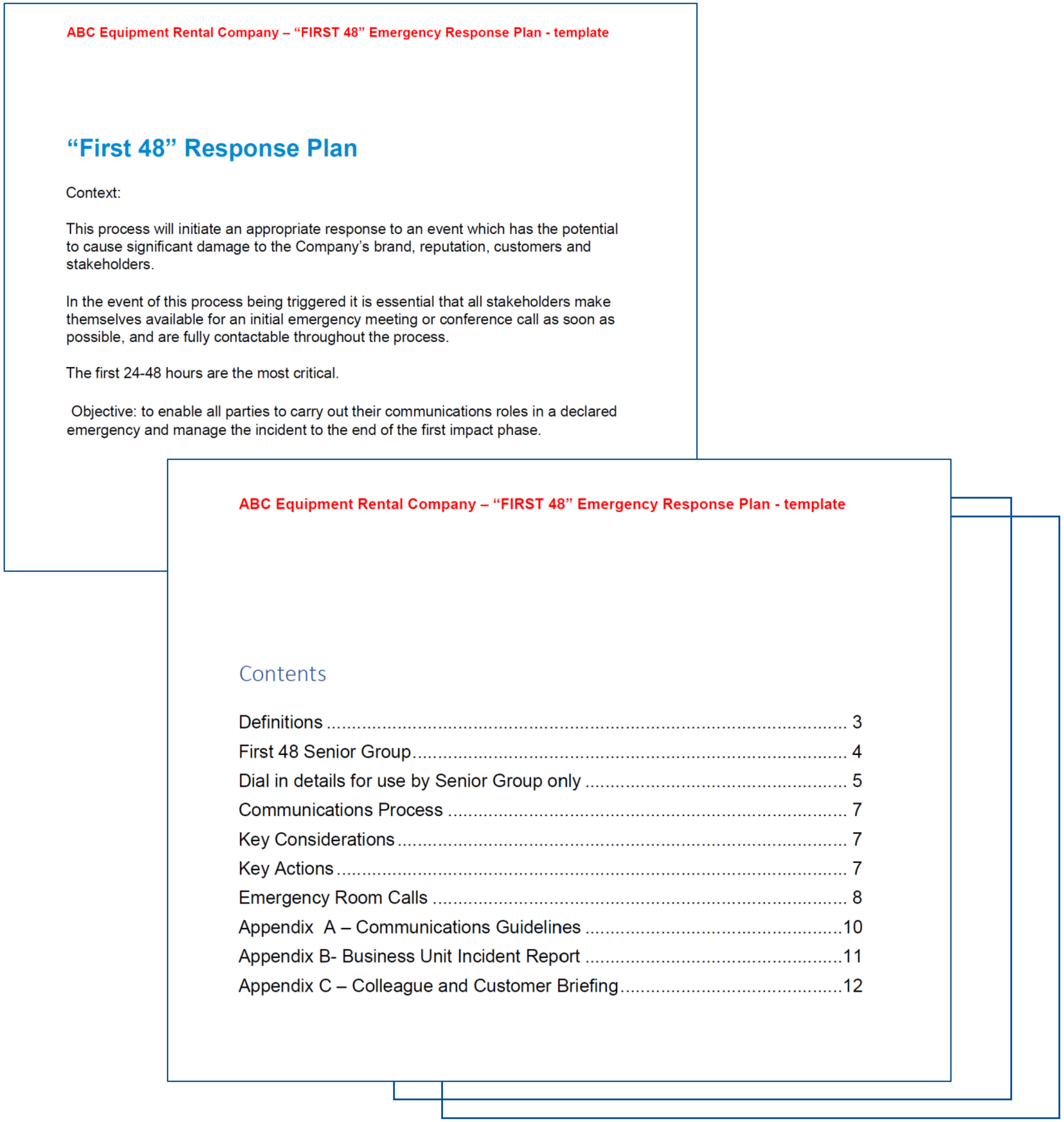
1. Enterprise-wide cybersecurity: risk assessment checklist

See (Word.doc)

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							
Cyber Security Plan and Investment	✓				✓		1
Risk Assessment							
Industry Frameworks and Standards							
Governance							
Continuous Improvement /Horizon Scanning							
Other?							
People							
Enterprise-Wide Awareness							
Training and Development							
Roles and Responsibilities							
Monitoring and Coaching							
Cyber Security 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. “First 48” response plan

See (Word.doc)



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

References and acknowledgements

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

References used in this guide include the following:

Context	Origin	Reference
Worldwide cybersecurity statistics	Gartner Cybersecurity Ventures Verizon	Gartner Cybersecurity Ventures Verizon
European cybersecurity Legislation	EU NIS directive	Directive on security of network and information systems
Cybersecurity trends	Gartner	IT Key Metrics Data 2019: Key IT Security Measures: by Industry (gartner.com)
Cybersecurity trends	Cyber-observer.com	29 Must-know Cybersecurity Statistics for 2020 - Cyber Observer (cyber-observer.com
Cybersecurity best practices	National cybersecurity Centre, UK	About Cyber Essentials - NCSC.GOV.UK
Cybersecurity best practices	Center for Internet Security	Cybersecurity Best Practices (cisecurity.org)
Threat and health monitoring	Microsoft.com Splunk.com	Azure Sentinel – Cloud-native SIEM solution | Microsoft Azure Enterprise Security Solutions | Splunk
"OSINT" for Digital Asset Discovery - "Open Source Intelligence	Wikipedia	Open-source intelligence - Wikipedia
The "Internet of Things" (IoT)	Wikipedia	Internet of things - Wikipedia

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).
Version 1: June 2021

Disclaimer:

This Guide represents data, research, opinions or viewpoints published by ERA - the European Rental Association and are not representations of fact. The information and opinions expressed in this publication are subject to change without notice and ERA - the European Rental Association have no duty or responsibility to update it. Moreover, while the materials reproduced herein are from sources considered reliable, the accuracy and completeness thereof are not warranted, nor are the opinions and analyses which are based upon it. To the extent permitted by law, ERA - the European Rental Association shall not be liable for any errors or omissions or any loss, damage or expense incurred by reliance on materials or any statement contained in the publication, or resulting from any omission.