EUROPEAN
RENTAL
ASSOCIATION

EXECUTIVE SUMMARY
ERA guide to cybersecurity leading practice in the equipment rental industry

Cybersecurity - are you equipped for the challenge?

One of the greatest threats to the equipment rental 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 interventions, 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 compiled with the invaluable support and contributions of ERA member companies.

The cybersecurity threat today and the "call to action"

This Guide outlines how the equipment rental sector across Europe faces an unprecedented challenge in the threats posed by information technology vulnerabilities and exposures in our business, and particularly how customers are demanding more and more from us on cybersecurity protection. The industry is in a process of consolidation, with 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 means more cybersecurity threats. Equipment for rental is becoming more and more intelligent and connected to networks, which can be the conduit for attack. 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. EU legislation is increasing in intensity and the Guide points to the latest developments in the EU NIS (Security of Network and Information Technology) Directive. The industry now needs an ongoing community amongst European companies to collaborate on cybersecurity best practice, common threats and issues facing all organisations.

Cybersecurity budgeting and investment needs

This Guide illustrates the investments in, and costs of, getting cybersecurity right. It presents a scale of investment and "maturity" indicating initial investment to get basics in place. Good cybersecurity requires significant investment - and must be renewed each year. Direct investment in cybersecurity across all industries is quoted as around 5% of IT spend, with more at the outset. Leaders also show that the larger investment is in indirect and intangible costs of "designing in", managing and embedding security into everything they do, which may ultimately amount to more than the direct costs.

Roadmap of leading practices and "Checklist"

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 and Infrastructure and so this Guide analyses them and presents core capability requirements at each of three levels of "Base Level", "Maturing" and "Leader". A checklist is included which links the essential risk and vulnerability assessment with current levels of maturity in the business as an aid to planning and risk reduction.

"You get what you measure….." Leaders report that it is essential to ensure key areas of performance that impact cybersecurity status are measured with Key Performance Indicators (KPIs). The Roadmap in the guide goes on to indicate typical measures and performance measurement systems in use today by leader companies for each of the elements.

Leading Practices Illustrated

This Guide then illustrates some of the leading practices in use today against the four capability elements. 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. Key features include:

- **Process**: 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. Leaders 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 in use are outlined.

- **People:** *Cybersecurity is not an "IT thing"…* There is an important role for Human Resources Management (HR) in cybersecurity defence. The scope of HR intervention and support in Leader companies is enterprise wide, across 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, awareness and training on cybersecurity imperatives and training needs analysis for front line roles and specific security personnel. Communications media such as newsletters or social media bulletins to broadcast latest trends or threats across the enterprise are essential.

- **Technology:** Information technology tools continue to develop rapidly and provide a powerful means of cyber defence, for "early warning" and threat interception. Threat and Health Monitoring is enabled by technology with advanced systems such as "Splunk" and "MS Azure Sentinel" illustrated in use. Establishing a "SOC" (Security Operations Centre) is shown as 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.

- **Infrastructure:** *"If the worst happens, despite all the best prevention measures, you have to be ready with an Incident Management Plan."* 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. This Guide illustrates how leaders analyse and respond and provides a "first 48" template, which can help to plan for the crisis management period immediately following a systems denial event or other major failure threat.

Prepare for a secure future

The race for good IT security will never end, but to stay ahead, leaders stress that 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 'ERA guide to cybersecurity leading practice' aims to help equipment rental companies of all types and sizes plan for, develop, or continuously improve their cybersecurity.