EUROPEAN
RENTAL
ASSOCIATION

Guide to Cybersecurity leading practice

David RILEY,

DKR Projects

Please react on Twitter, @era_rental, #eraconvention2021

A guide to cybersecurity leading practice in the equipment rental industry

Are you equipped for the challenge?

Please react on Twitter, @era_rental

A guide to cybersecurity leading practice in the equipment rental industry

DKR Projects

David Riley

Director, DKR Projects Ltd

- *Working with global industries on the development of Best Practice Processes*

Our role in this project - To work with ERA, its members and its cybersecurity working group to develop a new guide.

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

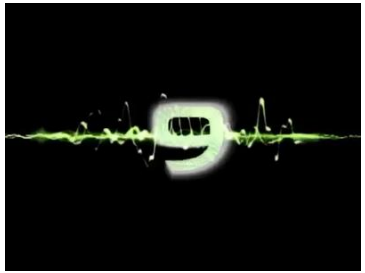
LOXAM, mateco, renta, HSS Hire, RIWAL, Boels RENTAL, KILOUTOU, CGT A TESYA COMPANY

To download the guide :

- search for “ERA guide to cybersecurity leading practice”
- or go to https://erarental.org/publications/

One of the greatest threats to our industry is the vulnerability to cybersecurity impacts on our businesses… Why?

Because, according to Google, just in the month after our guide was prepared, there were 86 reported incidents, with 34 million data records breached.



Because, last year there was a cyber attack …

every 14 seconds ...

this year every 9 seconds …

next year? … every 5 seconds?

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

Last year….

- 71% of breaches were financially motivated, 25% were motivated by espionage.

All equipment rental companies use some, or all, of these channels so everyone, *regardless of size and maturity in our industry,* is at risk.

In 2021, there is no established cybersecurity practices roadmap in our industry..

… Where an equipment rental company can:

- evaluate where it stands
- identify leading practice it can aspire to.

So, the guide sets out to:

- define the enterprise-wide scope, including special factors
- outline leading practices being adopted today by leaders in our industry.

…. And offer insights and a “Roadmap” for good security, focused on our particular sector ...

The guide contents cover ….

The cybersecurity landscape for our sector	The cybersecurity threats today and the “Call to action”
Investment levels required	Ongoing cybersecurity budgeting and investment needs
Roadmap of leading practices and “Checklist”	A planning “Roadmap” for cybersecurity risk and prioritisation
Leading practices illustrated	Basic, advanced and leader practices, illustrating the roadmap
Useful templates and tools	Examples of leading practice in useful guides and templates

To download the guide :

- search for “ERA guide to cybersecurity leading practice”
- or go to https://erarental.org/publications/

In summary .....

The cybersecurity landscape for our sector	The cybersecurity threats today and the “Call to action”
Investment levels required	Ongoing cybersecurity budgeting and investment needs
Roadmap of leading practices and “Checklist”	A planning “Roadmap” for cybersecurity risk and prioritisation
Leading practices illustrated	Basic, advanced and leader practices, illustrating the roadmap
Useful templates and tools	Examples of leading practice in useful guides and templates

Some key messages came out of the research and are explored in the guide, including ….

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 … 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.
  - "Hub and spoke" – protected centre, exposed depots
- Our equipment for rental is becoming more and more intelligent and more of it is connected to networks. Telematics and GPS used to geolocate and steal equipment.
- The equipment rental business is embracing "Digitalisation". More online interaction means more cybersecurity threats.

Views of equipment rental Leaders…

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.

"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 their customers at high risk.

Insights from some equipment rental "Leaders" are explored in the guide, including ….

"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, 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 by each organisation via a **risk assessment** across their estate."

Insights from 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 threats – *Special factors …*

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.

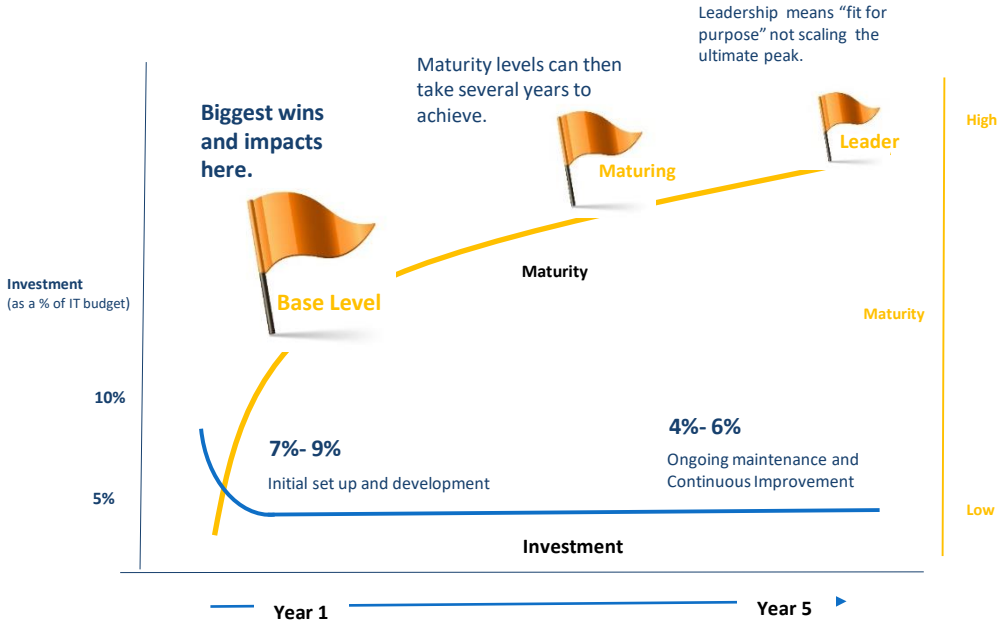
Since day 1, bringing people along with us was a matter of pragmatic common sense. We said to ourselves "You would not design a depot layout without a fence round it and strong locks on the gate. And it would have an intruder alarm system and cameras monitoring it. Why would you ever think it acceptable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

Guide contents

The cybersecurity landscape for our sector	The cybersecurity threats today and the “Call to action”
Investment levels required	Ongoing cybersecurity budgeting and investment needs
Roadmap of leading practices and “Checklist”	A planning “Roadmap” for cybersecurity risk and prioritisation
Leading practices illustrated	Basic, advanced and leader practices, illustrating the roadmap
Useful templates and tools	Examples of leading practice in useful guides and templates

The guide considers key factors in “Investment and Maturity”

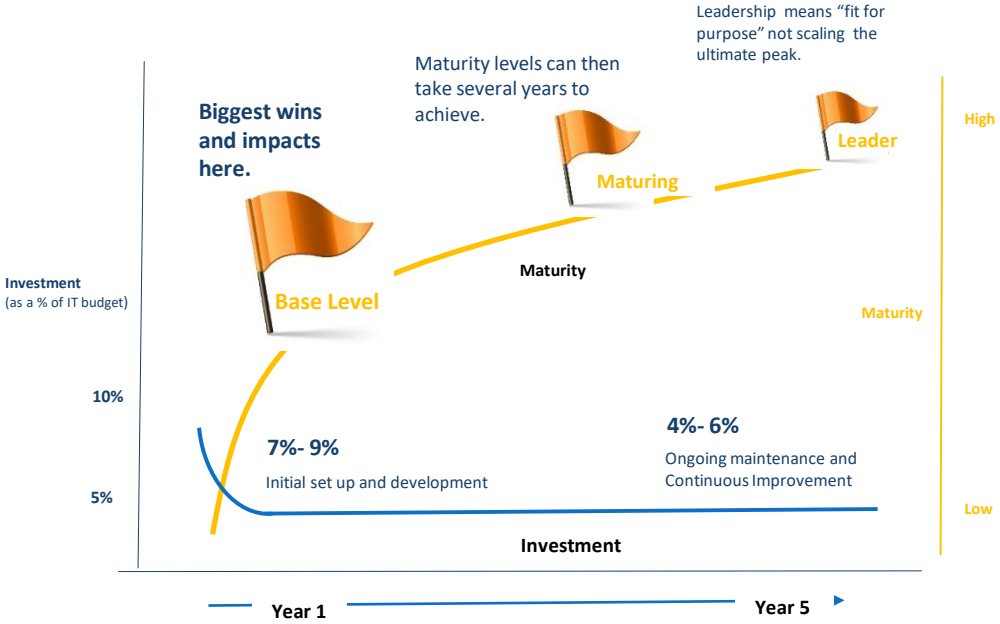
- Good cybersecurity requires significant investment, renewed each year. A common benchmark for **direct** investment in cybersecurity across all industries is quoted as **4-6%** of IT spend.
- Larger investment is in **indirect and intangible** costs of “designing in”, managing and embedding security into everything they do, which may ultimately be more than the direct costs.



The guide considers key factors in “Investment and Maturity”

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.”



Guide contents

The cybersecurity landscape for our sector	The cybersecurity threats today and the “Call to action”
Investment levels required	Ongoing cybersecurity budgeting and investment needs
Roadmap of leading practices and “Checklist”	A planning “Roadmap” for cybersecurity risk and prioritisation
Leading practices illustrated	Basic, advanced and leader practices, illustrating the roadmap
Useful templates and tools	Examples of leading practice in useful guides and templates

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

Process

People

Technology

Infrastructure

Whilst each company will have different approaches and priorities, the guide offers a four factor model as 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

The guide details each “Maturity stage” by element and offers a template for a risk assessment

Features of each maturity level:

Process
People
Technology
Infrastructure

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.

Analysis by factor then feeds into a risk assessment

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							

Guide contents

The cybersecurity landscape for our sector	The cybersecurity threats today and the “Call to action”
Investment levels required	Ongoing cybersecurity budgeting and investment needs
Roadmap of leading practices and “Checklist”	A planning “Roadmap” for cybersecurity risk and prioritisation
Leading practices illustrated	Basic, advanced and leader practices, illustrating the roadmap
Useful templates and tools	Examples of leading practice in useful guides and templates

The guide illustrates some leading practices in each of the four factor areas

Leading Practices - Process - Enterprise-wide accreditation frameworks

Process ✓
People
Technology
Infrastructure

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

ISO 27001 Certified

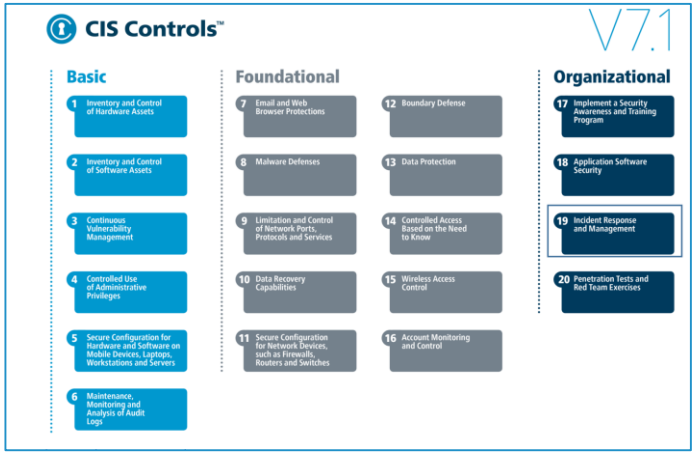
ISO27001 is an international standard on how to manage information security

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.



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

The guide illustrates some leading practices in each of the four factor areas

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

Process
People ✓
Technology
Infrastructure

Train in the essentials and generate awareness first. Low cost, high impact.

Embed cybersecurity into the organisation and all roles, enterprise-wide.

Measure and test people’s compliance, understanding and effectiveness.

Increasing maturity

“Behaviour and behavioural change is probably the single lowest cost, highest impact risk area to address ...”

“... Behavioural change takes time and is difficult.”

Leader insights: the guide illustrates some leading practices in each of the four factor areas

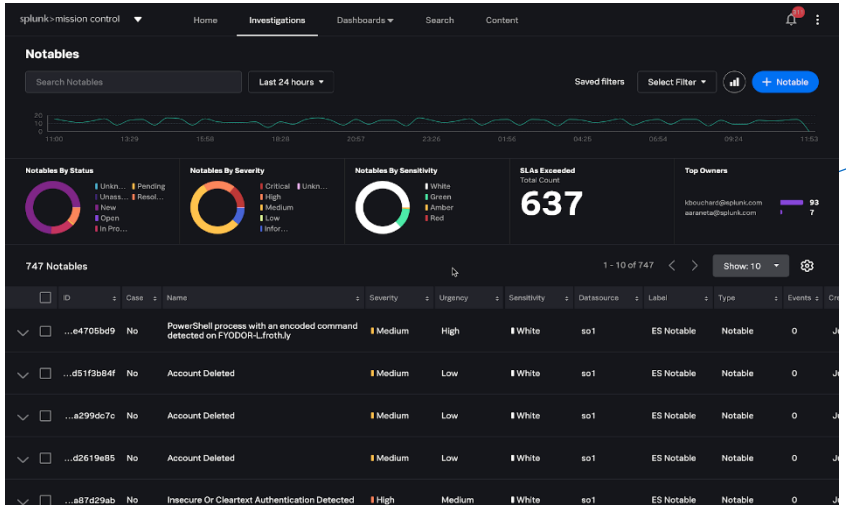
Process

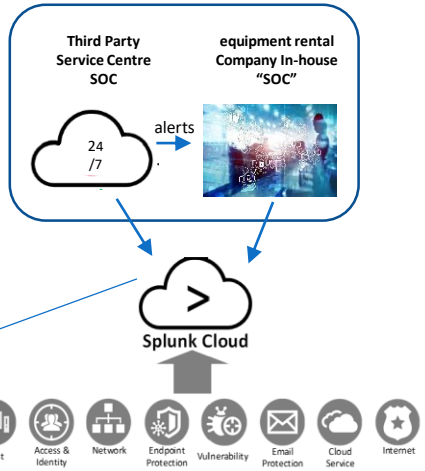
People

Technology ✓

Infrastructure

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





- 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.

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*

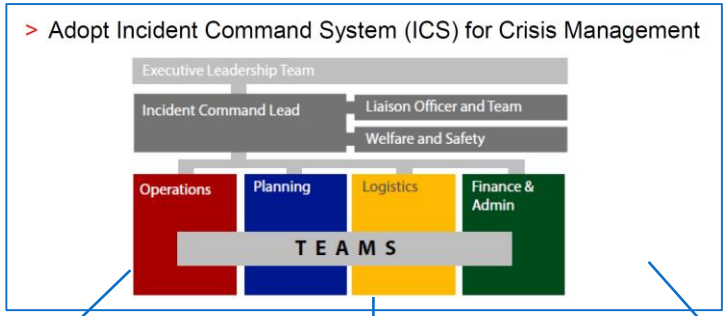
*Refer to: Enterprise Security Solutions | Splunk

Leader insights: the guide illustrates some leading practices in each of the four factor areas

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



- 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

Leader insights: the guide illustrates some leading practices in each of the four factor areas

Process

People

Technology

Infrastructure ✓

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

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

"Ransomware attack" ?

Assess and "Triage" the situation:

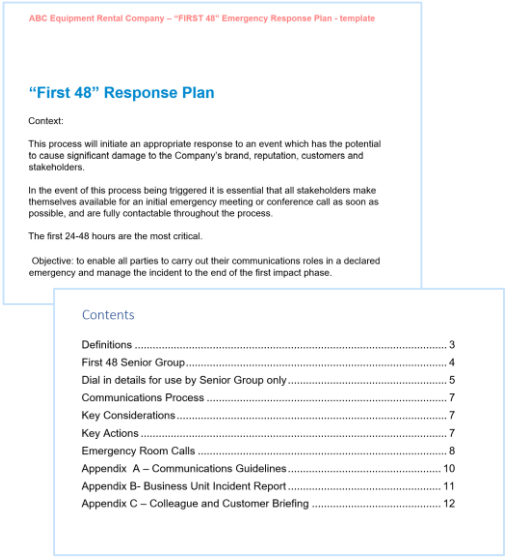
- Does this incident merit classification as an emergency?
- Is it ongoing? Should emergency response Plans be activated now?
- Who can authorise disconnection from the network, the internet and closedown of a system that writes business?
- When will that permission to act be empowered?
- When will that 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.

The guide offers a "First 48" plan template



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

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.”*

To download the guide :

- search for “ERA guide to cybersecurity leading practice”
- or go to https://erarental.org/publications/

Please react on Twitter, @era_rental

DKR Projects

Contact: David Riley

driley@dkrprojects.co.uk