CDOIF

Chemical and Downstream Oil Industries Forum

Guideline

Cyber Security for Senior Managers

Foreword

In promoting and leading on key sector process safety initiatives, CDOIF has developed through its members this guideline to assist senior managers in understanding cyber security.

It is not the intention of this document to replace any existing corporate policies or processes.

There are no limitations on further distribution of this guideline to other organisations outside of CDOIF membership, provided that:

1. It is understood that this report represents CDOIF’s view of common guidance on cyber security for senior managers.
2. CDOIF accepts no responsibility in terms of the use or misuse of this document.
3. The report is distributed in a read only format, such that the name and content is not changed and that it is consistently referred to as "CDOIF Guideline – Cyber Security for Senior Managers".
4. It is understood that no warranty is given in relation to the accuracy or completeness of information contained in the report except that it is believed to be substantially correct at the time of publication.

This document does not explore all possible options for demonstrating compliance against relevant cyber security regulatory instruments, nor does it consider individual site requirements – Following the guidance is not compulsory and duty holders are free to take other action.

For the purpose of regulation, the Health and Safety Executives current interpretation of relevant good practice for compliance is found in OG 86 *Cyber Security for Industrial Automation and Control Systems (IACS)* – this CDOIF publication provides additional guidance on governance.

Contents

1. EXECUTIVE SUMMARY

Cyber-attacks are becoming more common, and with greater automation and interconnectivity between systems, these attacks are a significant risk to business. There have been several high-profile incidents in recent years, including those on the National Health Service and the Ukraine power network. Recent research published by an insurer indicated that over 60% of firms had reported an attack in 2019[1], up from 45% in 2018. These figures suggest that businesses should assume that they have, are, or will shortly be attacked.

Computer systems are integral to everyday operations and are often used in many different applications including industrial control and automation systems, email and document services, power management, buildings management and telephone systems. A convergence of technologies has meant that these different applications can run on the same computers and networks, reducing costs for business, but potentially exposing sensitive systems to attack. Any business can be targeted – size and function are unimportant.

Cyber security is a high priority for Government. The Health and Safety Executive (HSE) has been active at operational level and now includes cyber security within their front-line intervention activities.

This guidance provides a summary of why cyber security is a risk to safety for all chemical and downstream oil industries. There are additional requirements under the Control of Major Accident Hazards (COMAH) Regulations, and in the context of the Network Information Systems (NIS) Regulations, security of essential services.

The guidance provides advice for senior managers to ensure that risks are being managed and minimised. In doing so business will also reduce risk to commercial activities and protect their reputation, this guidance includes:

- Governance: Roles and responsibilities, reporting, accountability, organisation structure, vision and culture.
- Staff competencies: Knowledge, skills and experience.
- Management system documentation: letting people know what's required.
- Audit of management systems and technical aspects, and monitoring of key performance indicators: making sure procedures and countermeasures keep working.
- Managing supply chain risk.

This guidance is principally aimed at Industrial Automation and Control Systems (IACS) but many of the principles also apply to the corporate Information Technology (IT) system

[1] HISCOX Cyber Readiness Report 2019

2. TARGET AUDIENCE

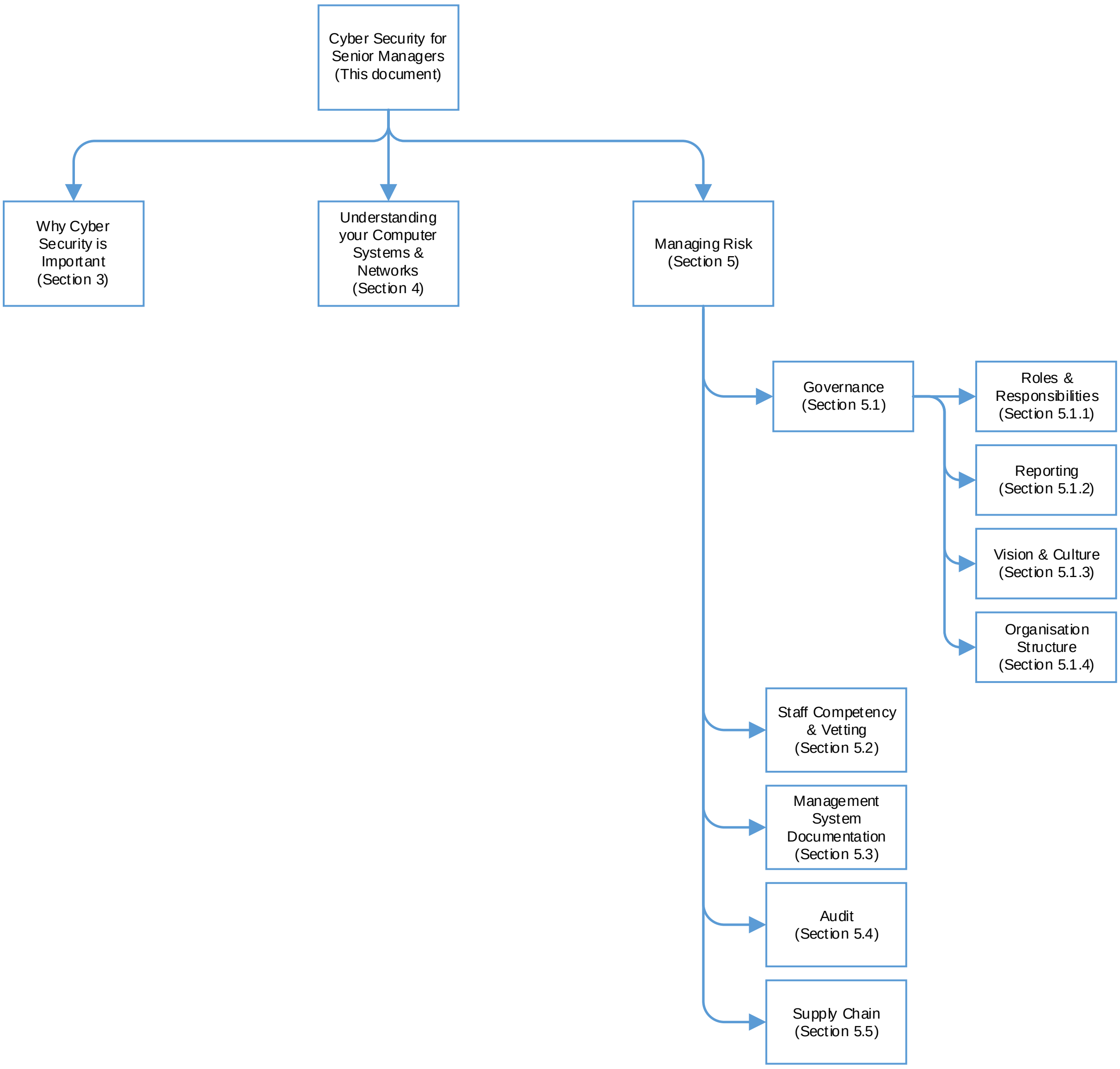
This guidance has been written for senior managers; this includes:

- Board, executive team / senior management team.
- Facility owners who employ others to operate and maintain their facilities.

Other personnel within the business may find this guidance useful, such as:

- Site managers and engineering managers.
- Operational staff to assist in their dialogue with senior managers.
- Other site-based personnel without specific cyber security knowledge.

2.1 Using this Guidance



Cyber Security for Senior Managers (This document)
Why Cyber Security is Important (Section 3)
Understanding your Computer Systems & Networks (Section 4)
Managing Risk (Section 5)
Governance (Section 5.1)
Roles & Responsibilities (Section 5.1.1)
Reporting (Section 5.1.2)
Vision & Culture (Section 5.1.3)
Organisation Structure (Section 5.1.4)
Staff Competency & Vetting (Section 5.2)
Management System Documentation (Section 5.3)
Audit (Section 5.4)
Supply Chain (Section 5.5)

Figure 1 – using this guidance

3. WHY IS CYBER SECURITY IMPORTANT TO YOU?

Recent cyber-attacks have shown the impact on businesses in terms of:

- Industrial liabilities
  - Loss of life
  - Damage to the environment
  - Loss of production
- Costs
  - Loss of customers
  - Technical fix
  - Long term measures – media responses etc
- Criminal proceedings against business and individuals
- Loss of reputation

Case Study – Schneider Electric

In August 2017, a cybersecurity event compromised the automation systems of a Middle East refinery. The malicious malware recovered from the system became known as Triton, Trisis or Hatman.

Analysis indicated a security Level 4 (nation state) attack had been ongoing for multiple years, with the Enterprise layer, Control layer and finally the Safety layers all being compromised. Fortunately, the safety system (the last line of defence protecting against hazardous conditions) detected an anomaly and a safe plant shutdown was initiated.

The cyber-attack was complex in nature and was coupled with a series of lapses in the on-site Cyber security procedures. The full potential of the attack was not realized, the intent is not known but the possibility of full command of the control and safety systems, could have had severe consequences to the plant, people and the environment.

A cyber forensic response team was mobilized acting in accordance with its pre-prepared Cyber Incident Response Plan, to respond to the immediate site incident and to react quickly to media inquiries and coverage in the days following the disclosure. The team also engaged with many stakeholders, including internal teams, forensic investigators, government agencies and industry analysts.

The necessity to be prepared with a response plan, including the expertise required to respond to the incident, perform the forensic investigation, analyse and communicate the facts with all the concerned parties, cannot be underestimated.

The plan should also include measures to combat the inaccuracies and sensationalism reported by the media and competitors (which is significant) and companies seeking to gain advantage from the situation and sell technology and services without a full appreciation of the FACTS.

The initial months of response were all consuming for many employees but what cannot be underestimated is the slow burn over the next two years and the years to come. Articles are written, presentations are made by people without the full knowledge, that must be replied to, to maintain product and company integrity. Any cyber incident renews interest.

Cyber attackers are becoming bolder. This underscores Schneider Electric’s efforts to continue to focus on cybersecurity and defence-in-depth measures. Operating companies should recognize that an industrial control and automation system-focused approach to securing their site must also be taken.

Finally, had the documented security procedures for the safety system been followed, the safety system would not have been compromised. This highlights the need for strong relationships with vendors to install, commission and maintain their systems and to supply the immediate response and cyber expertise, should it be required.

Attacks may impact the IACS of the business. This could result in unauthorised changes, removal of safety features, loss of control or visibility and an increase in process risk - resulting in production downtime, quality issues or dangerous occurrences. In some instances, an initial breach in security may not be detected for days, weeks, months or years later.

Case Study – Norsk Hydro

In early 2019 a ransomware cyber-attack occurred at Norsk Hydro - 22,000 computers were impacted across 170 different sites in 40 different countries. The entire workforce had to revert to using pen and paper, and production lines switched to manual operation, or stopped altogether. In June 2019 the business was still working toward a full recovery, with costs of £45M.[2]

Case Study – Water Company

Water Company – Chemical Dosing Incident. Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water as well as gaining access to personal information of the utility's 2.5 million customers. This case highlighted aging systems' vulnerabilities and issues with security of the internet interface and subsequent links to the process control systems. The hackers first took control of the company's online payment application and gained access to all of the customers' financial data. They were also able to recover connection data for an administrator's account and the IP address of the server managing the industrial process. That enabled access to the infrastructure control interface and in turn allowed the hackers to modify the level of chemicals used in the water treatment process.[3]

In many countries there will be legislative instruments in place to ensure that businesses protect against attacks:

- In the UK, the COMAH Regulations 2015 requires businesses regulated under this legislation to prevent major accidents involving dangerous substances and limit the consequences to people and the environment of any accidents which do occur. Failure to demonstrate this could result in improvement or prohibition notices, or significant fines on the business.[4]

- In 2018 the UK adopted the NIS directive as the NIS Regulations. This places additional responsibilities on businesses which are designated as Critical National Infrastructure (for example heath, transport, oil and gas providers). The directive applies to IACS and business systems. Failure to demonstrate that these systems are adequately protected can result in significant penalties being imposed.[5]

- The functional safety standards (IEC 61508 and IEC 61511) include requirements for safety related systems to be protected against cyber-attack.

Regardless of whether a business is regulated under COMAH or the NIS regulations, managing cyber risk is good business. The size and nature of a company is not a barrier to attack – all businesses are at risk. **All companies need to ensure that they understand how they are at risk and from whom – and ensure appropriate and proportionate safeguards are in place.**

[2] BBC Business 'How a ransomware attack cost one firm £45m'
[3] The Register 'Water treatment plant hacked, chemical mix changed for tap supplies'
[4] OG 86, Cyber Security for Industrial Automation and Control Systems (IACS) ed 2
[5] The Network and Information Systems Regulations 2018

There are many different sources of a potential cyber incident, including threats from within a business (accidental of deliberate).

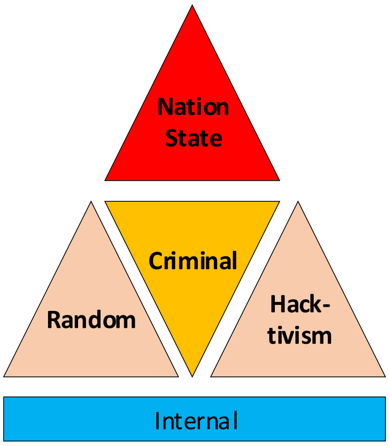


Figure 2 – Sources of Cyber Attacks

Further information regarding how cyber-attacks occur can be found on the National Cyber security Centre website “How cyber attacks work”.

4. UNDERSTANDING YOUR COMPUTER SYSTEMS AND NETWORKS

Computer systems are an essential part of business infrastructure, the use of which can improve performance and reduce costs. Some of these systems, if compromised, could have an adverse safety impact on the business. It is the responsibility of the board and senior management team to ensure that these systems are protected.

There are many different types of systems and external users and connections within a business, for example:

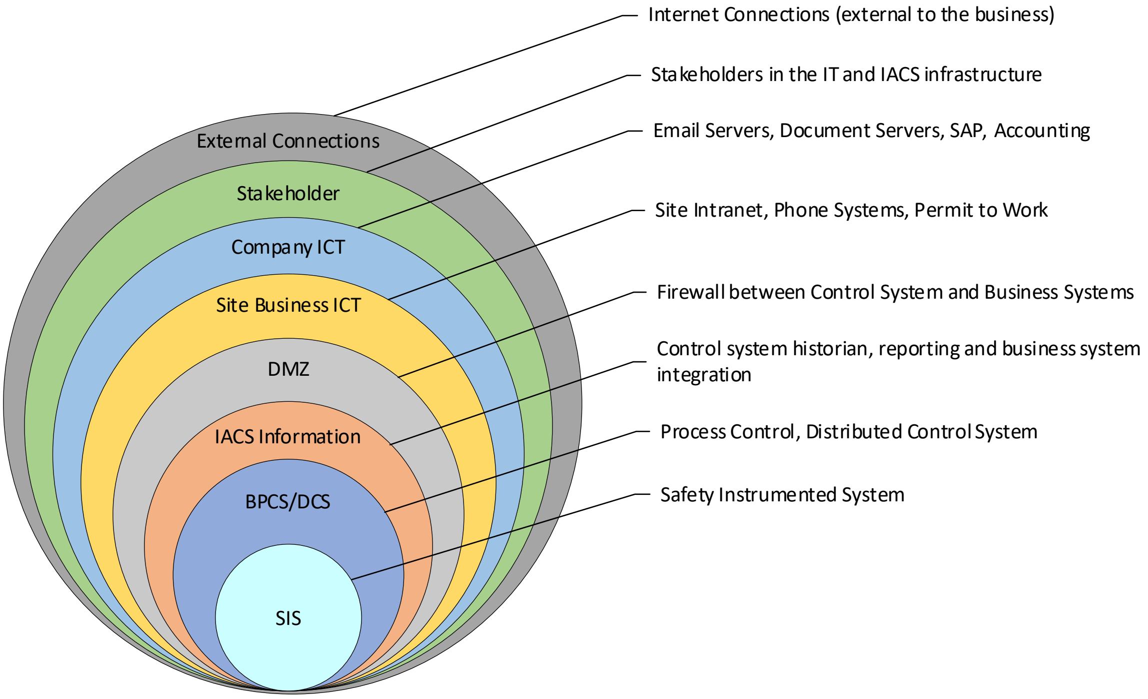

Internet Connections (external to the business)
Stakeholders in the IT and IACS infrastructure
Email Servers, Document Servers, SAP, Accounting
Site Intranet, Phone Systems, Permit to Work
Firewall between Control System and Business Systems
Control system historian, reporting and business system integration
Process Control, Distributed Control System
Safety Instrumented System
External Connections
Stakeholder
Company ICT
Site Business ICT
DMZ
IACS Information
BPCS/DCS
SIS

Figure 3 – Infrastructure Layers

Note: this diagram is not intended to be a representation of IT and IACS architectures, but simply to show the different systems that a business may have.

Industrial Automation, Process Control, Distributed Control, Electrical Control and Safety Systems that control plant and process and the assets that protect these systems are commonly referred to as the Industrial Automation and Control Systems - IACS (also known as Operational Technology - OT).

Note: there should always be a clear demarcation between IT / IACS.

Differentiation of the IACS from the IT systems is necessary as part of a defence in depth approach and so that access can be restricted, and proportionate cyber security countermeasures be applied.

However essential data resident on the IT network may also present a direct hazard to plant and processes when attacked. For example:

- Permit to work systems which are typically used to authorise maintenance activities on plant and process, and

- Shift handover systems used to communicate important plant information during a shift change.

Business therefore need a method to operate safely if essential data on the IT system cannot be accessed.

The integration of IACS and IT usually still represents a challenge due to the differences between them. For example, the lifetime of IT assets is usually 3-5 years, while the lifetime of IACS is 15-20 years.

These IT and IACS systems may reside on physical servers within company buildings, or they may be outsourced to off-site service providers, or even accessed via cloud computing.

An example of the complexities of a medium sized network is provided in the diagram below:

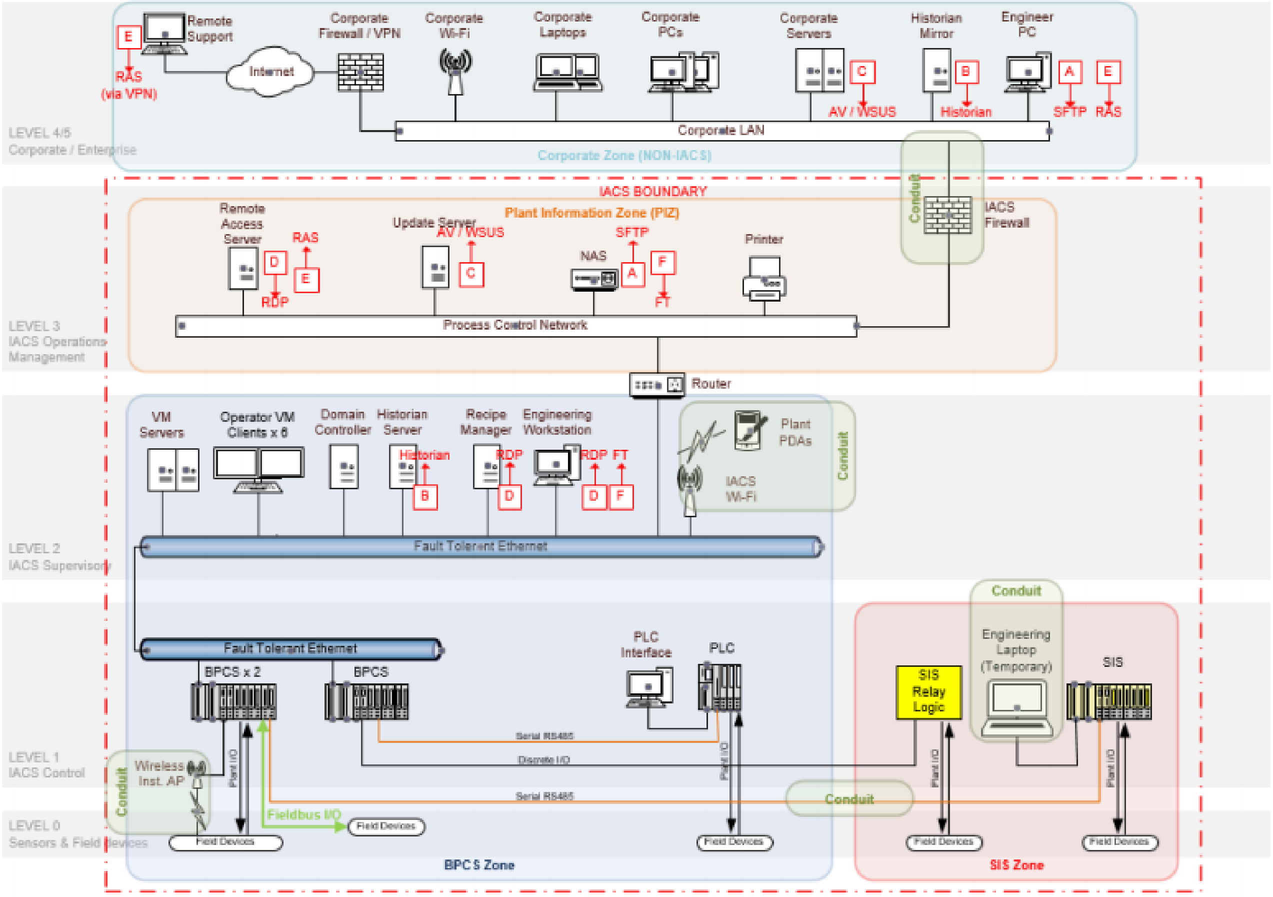


Figure 4 – Example network drawing medium sized site[6]

When defining and reviewing appropriate protection measures against cyber-attack, it is first important to know what is to be defended. The connectivity between each infrastructure layer needs to be risk assessed and mitigated. Robust response and recovery plans should be developed and tested.

[6] OG 86, Cyber security for Industrial Automation and Control Systems (IACS) ed 2

> *Industrial Automation and Control Systems (IACS) are often integrated with business systems such as finance, ordering, or enterprise resource systems to improve company performance.*

Protection against a major accident relies both on the prevention, detection and mitigation of a cyber-attack and on plant safety related systems that do not pose a cyber security risk, for example: mechanical or hard-wired safety related systems.

It is also important to understand who has access (both physically and digitally) to what, and for what purpose, so that risks to systems can be managed appropriately. This requires support people who have IACS as well as IT skill sets.

Further information on understanding computer systems and networks can be found in the useful resources section of this guidance.

5. MANAGING RISK

It is important that the business understands what needs to be protected and the risks that a cyber-attack can cause.

It is expected that the business carries out a review to identify corporate responsibilities, vulnerabilities, consequences and to highlight where improvements need to be made. This will also include carrying out any necessary risk assessment as an ongoing process.

For further information about carrying out risk assessments refer to OG 86, NIST SP 800-82, IEC 62443 (refer to References).

> *The OG 86 approach to risk assessment seeks to identify for each asset zone, the consequences of a cyber-attack and the criticality of the assets in preventing these consequences.*

The following sections provide further information on how risks can be mitigated.

5.1 Governance

5.1.1 Roles and Responsibilities

The board or Senior Management Team (SMT) has responsibility for physical and digital security.

Further responsibilities include:

- People, ensuring appropriate resource and competency, and effective communication

- Process, ensuring corporate risk registers, management and audit systems cover cyber security

- Technology, ensuring appropriate technology is deployed and regularly updated

For further information refer to IEC 62443, ISO 27001/2, World Economic Forum ‘Advancing Cyber Resilience Principles and Tools for Boards’.

5.1.2 Reporting

Performance Indicators

Performance indicators provide confidence that the businesses cyber security management system is effective and provide information about potential areas of improvement.

Some organisations may want to use the HSG254 model of Leading and Lagging indicators, but there are other models available. The most important thing is to identify useful performance indicators and to act on them. Examples of typical performance indicators are given in Appendix 1.

IACS specific performance indicators should be developed because, for example:

- IACS security events should be less frequent but will be more important

- the IACS is likely to have outstanding (unpatched) vulnerabilities due to longer IACS lifecycles (obsolescence)

- delays caused by assurance steps taken before deploying fixes into the IACS.

Relevant performance indicators should be presented to the SMT or at board level. Where weaknesses are identified, the board should ensure that appropriate improvement plans, and resources are put in place. Any action plan should be monitored to completion.

Speculative Information

Performance indicators can only measure pre-determined parameters. To avoid rigidity in this system you also need access to speculative information, for example:

- Internal/External intelligence

- Media reports and/or interest

Metrics change over time and according to circumstance, so assessing performance indicators value for the organisation will be an ongoing process. High quality performance indicators can serve as a security programme enabler and driver for continuous improvement. However, the rate of change of the nature of technology and cyber-attacks make it essential that performance indicators are reviewed and refreshed on an ongoing basis.

Note that cyber-attacks are be reportable under COMAH and the NIS Regulations if they are above specified thresholds for safety and loss of services respectively.

5.1.3 Vision and Culture

Leaders should seek a balance between risk and benefit from a technical and business perspective, where:

- Cyber security risk is a business risk and therefore should be integrated into existing organisational risk management (operational, legal, financial)

- People have a good relationship with security and there are efficient processes

- Leaders engage with technical experts to establish objectives and improve communication with technical staff

- Responsibilities encourage all leaders to participate, and empower technology teams where appropriate

- Leaders should consider the results from the cyber security risk assessments and act on the findings where appropriate. This may include allocation and arrangement of resources

Good cyber security governance will rely on adequate information on which to base strategic decisions. Leaders should want to hear what is happening regarding cyber security risk and the dynamic nature of vulnerabilities, threats and organisational and technical countermeasures.

In order that information can be accessed and assessed quickly, leaders should:

- Ensure there are no barriers to the communication of bad news

- Consider how organisational structure, roles and responsibilities will filter information

- Ensure that incidents, near misses and external sources (for example media monitoring) on cyber events are considered and action taken as appropriate.

- Ensure that the reporting mechanism can keep pace with the changing nature of cyber threats

- Ensure effective communication with and across departments and technical teams

- Ensure effective communication with external stakeholders and peers (for example trade bodies/associations, customers, suppliers, and relevant government agencies)

The pace of environmental change (for example in vulnerability, threat and cyber integration with the business) will require a focus on building new competence as well as using existing competencies within the business. Senior managers will need to ensure that competence is addressed to ensure that relevant teams are sufficiently trained and informed to be reactive to new threats. This may require:

- Raising awareness of the common challenges across departments (for example operations, engineering and IT) and ensuring these teams collaborate

- Raising awareness of the value of collaborating externally (for example with trade bodies/associations, customers, suppliers, and relevant government agencies)

- Raising awareness that knowledge and training for cyber security changes quickly and goes out of date, it should therefore be addressed more dynamically.

People are at the heart of security. Leaders should engage with and respect security decisions and take responsibility for their own role, recognising that they will be targets due to their access and influence. As part of a concerted effort on culture, leaders should:

- understand the importance of people’s behaviours in ensuring cyber security

- ensure that people understand the risks and the importance of their actions.

- make sure security processes work for users and highlight ineffective procedures

- speak openly and positively to staff about cyber security

- ensure staff are empowered to raise security concerns via a suitable mechanism

- recognise that staff can provide an early warning and an opportunity for learning if the culture encourages them to speak out, and in particular:

  - people are not punished for reporting bad news

  - there is a mechanism available for business stakeholders to report incidents and people know how to report

  - the business has a no-blame culture (as for learning from health and safety incidents)

By developing a culture of trust and accountability, people can focus on learning and delivering benefit to the organisation rather than focusing on protecting themselves.

5.1.4 Organisation Structure, Strategy and Planning

Cyber security may not have previously been a consideration for business. Development of cyber security strategy should be integrated into the overall business strategy and be included in a mechanism to align business priorities and allocate investment.

Business strategy and organisational structure may need to be supplemented by additional arrangements to accommodate the faster pace of change, and the requirement for learning and new competency development.

Leaders should consider how the organisational structure may need to change for cyber security, including:

- the communication of cyber security information provided to leaders for decision making
- pace of decision making
- developing efficient communication between departments and with external stakeholders
- to improve the quality of communication between leaders and technical staff
- responsibilities, oversight and governance
- what objectives are set, by whom and at what level in the organisation they are set

Cyber security objectives should start to be established by identifying:

- corporate social responsibilities, legal and contractual requirements
- business priorities, which may be in terms of systems, data or services
- what technical and organisational changes are required to deliver these priorities

Leaders should consider that the needs of cyber security cannot be predicted with the same degree of certainty as physical assets, processes or markets. This is because cyber threats and vulnerabilities are continually changing.

Leadership will still want to set and achieve long term cyber security objectives (for example: on appetite for risk and to achieve a minimum level of IACS cyber security), however the leadership input to IACS cyber security strategy development may be to focus more on resources, relationships, communication, capability development and recognise that strategies can be effectively developed from lower levels within the organisation.

Some strategy development options are:

- legitimising strategies developed from lower levels within the organisation rather than top down decisions
- ad-hoc [e.g. on a project] cross-functional relationships (horizontal), for example IT to IACS and business to vendor, rather than traditional stable functional (vertical) relationships

- leader's attention on capabilities as well as goals
- reactive organisation capability as well as planned organisation for basic objectives

5.2 Staff Competency and Vetting

Many organisations will have Competency Management Systems (CMS)[7] in place to ensure that staff and contractors have the necessary competencies to manage operational activities, however this is unlikely to also include cyber security. Competence management for cyber security should be no different from competency management for other roles.

Senior managers should ensure that their CMS is reviewed and updated to include:

- the technical administration staff responsible for cyber security
- general awareness for users of IT and IACS systems
  - the National Cyber Security Centre (NCSC) provides free e-learning package[8]

When developing the CMS businesses should also consider:

- identification of tasks that may cause a cyber security risk, and the allocation of those tasks to roles and people.
- identification of tasks that are required to implement and maintain cyber security measures, and the allocation of those tasks to roles and people.
- identification of the competencies that are required to carry out these tasks, and any gaps and actions required to close these
- how cyber security threats and good practice are reviewed, and competencies updated as required (cyber security as a subject is rapidly evolving and so the CMS should be updated accordingly)
- what cyber security roles should be in house, and which are external services. Where external services are engaged, the business needs to maintain intelligent customer capability[9]. Reference should be made to section 5.5 for more information on the supply chain.

Where people have access to IT or IACS systems, senior managers should ensure that appropriate vetting is carried out due to the potential consequence of damage to the business.

- Vetting of staff should cover new employees and the movement of staff within the business and be proportionate to the access and risk of the role that they have.
- Vetting of contractors should also be required proportionate to the access and risk of the role that they have, or evidence is provided by the contracting company.

[7] Refer to the guidance listed in *Other Relevant Publications*
[8] NCSC's Cyber security training for staff
[9] Refer to the guidance listed in *Other Relevant Publications*

- Vetting alone may not be enough for highly sensitive tasks. Sharing critical roles within the business could improve security (for example requester and approver).

- Ad-hoc vetting of staff and contractors should also be carried out triggered by, for example, changes in behaviour.

The hierarchy of policies and procedures should facilitate the development of a CMS by identifying the key roles and responsibilities.

Case Study – Maroochy Shire Sewage Spill, Australia

A cyber insider attack - A contractor, previously working on the control systems of an Australian sewage treatment works, staged a series of hacking attacks after failing to get a permanent job at the site. The SCADA hack caused various pumping system control and alarm faults over a period of time and eventually resulted in millions of litres of raw sewage to spill out into local parks, rivers and the grounds of a Hyatt Regency hotel. Marine life died, the creek water turned black and the stench was unbearable for residents. The hacker received a two-year prison sentence.[10]

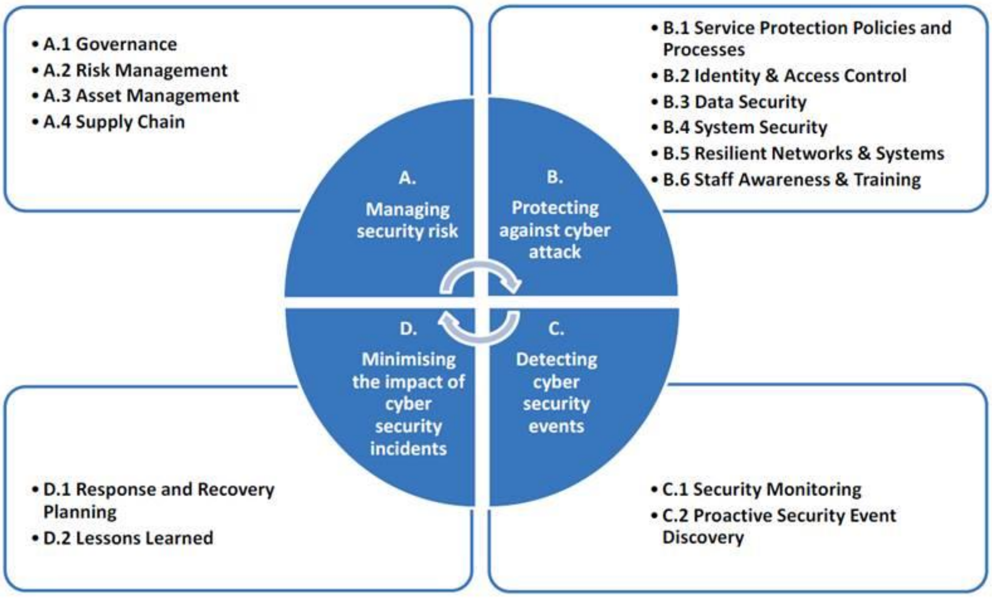
[10] The Register ‘Hacker jailed for revenge sewage attacks’

5.3 Management System Documentation

Policies, procedures, instructions and other documentation forming the cyber security management system should follow existing guidance on management systems, for example Plan, Do, Check, Act[11] and Management System Documentation[12]. These systems must be practicable and achievable and should be integrated into the businesses wider management systems.

When developing the cyber security management system, consideration should be given to:

- the four main topics of the cyber Assessment Framework (CAF)[13]:
  - Managing security risk
  - Protecting against cyber attack
  - Detecting cyber security events
  - Minimising the impacts of cyber security incidents



• A.1 Governance
• A.2 Risk Management
• A.3 Asset Management
• A.4 Supply Chain
• B.1 Service Protection Policies and Processes
• B.2 Identity & Access Control
• B.3 Data Security
• B.4 System Security
• B.5 Resilient Networks & Systems
• B.6 Staff Awareness & Training
A. Managing security risk
B. Protecting against cyber attack
D. Minimising the impact of cyber security incidents
C. Detecting cyber security events
• D.1 Response and Recovery Planning
• D.2 Lessons Learned
• C.1 Security Monitoring
• C.2 Proactive Security Event Discovery

Figure 5 – CAF Elements

- the separation of procedures between different infrastructure layers (refer to Figure 3), for example IACS will require different procedures to those of IT
- other management systems that may need to be updated to include cyber security. For example, Management of Change, risk assessment and the management of Safety Instrumented Systems through IEC 61511
- integration of cyber-attack response to existing emergency planning

[11] Managing for Health and Safety (HSG65)
[12] ISO/TR 10013:2001 Guidelines for quality management system documentation
[13] Cyber Assessment Framework

- good corporate governance split between technical and management systems[14]

- independent certification to ISO 270001, Information Security Management

- appropriate procedures for people leaving or moving within the business to ensure that access to IT and IACS systems has been removed.

Essential to any management system and its policies and procedures is the need to ensure an accurate and up to date inventory of IT and IACS. The inventory should consider all relevant partners and stakeholders. Management teams should also be aware of the risk from undocumented systems and workarounds.

Senior leaders should ensure that a cyber security management system is in place and is supported and resourced and that performance is audited, monitored and reported.

5.4 Audit

Audit provides senior managers with information relating to the effectiveness of the cyber security management systems, as well as the countermeasures that are in place to prevent or mitigate an attack.

Auditing should be differentiated between IACS and IT systems because requirements will be different. For example:

- Management system audit to ensure that the cyber security management system (refer to section 5.3) is both used as intended and is still appropriate for use.

    - This is a typical audit similar to those employed for safety, quality and environmental management systems.

- Technical audit which provide evidence of the existence of vulnerabilities and their ability to be exploited, as well as verify the ability of security countermeasures to prevent attacks or prevent errors. Technical audits are typically categorised as vulnerability assessment and penetration testing, both can identify failings in cyber security, however businesses should consider:

    - penetration testing, particularly for IACS, can be challenging and may cause unexpected impact such as shutdowns and system crash. Careful consideration should be given to whether this is required and the possible impact on production, safety and security.

    - the sensitivity of the technical audit and the use of authorised third parties to carry out work - the National Cyber Security Centre (NCSC) provides a register of authorised businesses that can carry out cyber security tests[15]

    - weaknesses in automated monitoring systems, which could include unintended impacts on devices or systems, such as shutdowns and system crash. Careful consideration should be given to whether these tools should be used and the possible impact on production, safety and security.

Existing auditing processes should be reviewed and updated to include the specific requirements for cyber security and related management systems. When developing the audit and monitoring systems, owners should ensure:

[14] OECD Corporate Governance
[15] NCSC Products and Services

- audits are carried out periodically or when a significant change or upgrade has been implemented (for example a configuration change on a critical countermeasure, such as a firewall or router)

- additional time is set aside for cyber security audits which can often take longer than traditional audits due to the technical aspects involved and may not be as mature as some other management systems

- appropriate levels of impartiality and independence of auditors.

- on completion the audit is correctly documented and circulated. Any actions arising should be traceable, implemented and verified. Senior leaders should be aware of audit results and any actions that are required

Further information is provided in HSE guidance on *Cyber security for Industrial Automation and Control Systems* (OG 86).

5.5 Supply Chain

Supply chain refers to contractors and vendors responsible for the supply of IT and IACS systems and services to the business.

Many threats and vulnerabilities relating to cyber security originate from the supply chain.

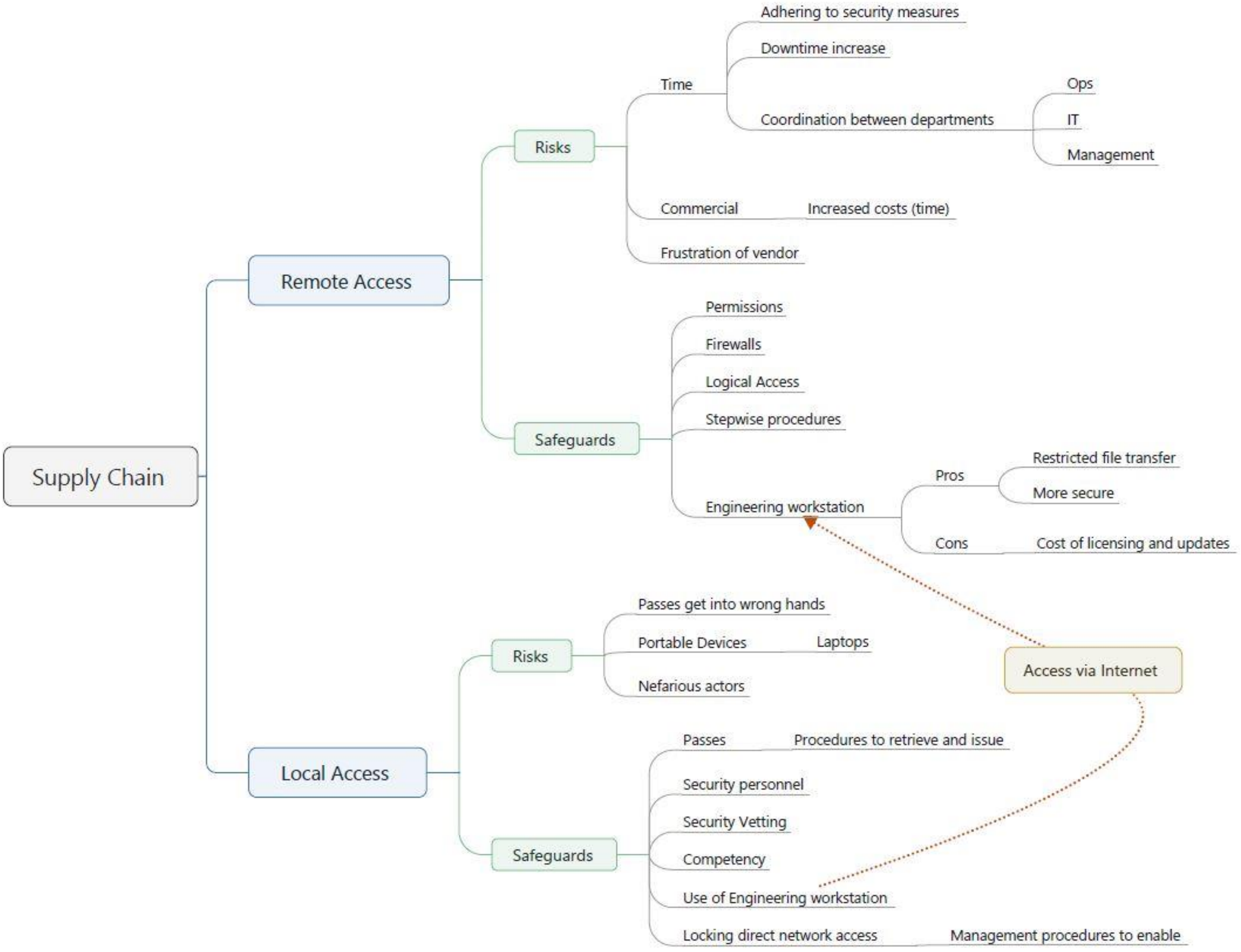


Figure 6 Example on and off-site vulnerabilities

- On site
    - Access control, for example passes, fobs, should be identified and managed
    - Systems to ensure that malware is not introduced to the businesses IT and IACS systems
        - Restrictions on the use of contractor's own equipment (software, data storage devices, IT equipment). For example, can you provide tools to allow the contractor to perform their work activity?
        - Control of the integrity of software update and validity mechanisms. For example, software patches and virus definitions
    - Seek assurance from vendors and third parties that appropriate controls are in place with regards to security vetting of employees. For example, through vendor checklists
    - Procedures for communications with contractors. For example, to protect against phishing emails
- Off site
    - Remote access has many benefits; however, these need to be balanced against the risks that may be introduced. The business will need to:
        - ensure the robustness of security measures in place for the contractor. For example, processes in place to prevent unauthorised remote access.
        - ensure only those systems that need external access have external access.
        - consider cloud and remotely managed services. These provide access to greater resources, however threats and benefits should be carefully assessed and considered within a risk assessment. For example, these are a high value target for a potential attacker. It is important that there is appropriate provision for the loss of such services at any potentially impacted site and level in the business.

Assurance for on site and off site measures for contractors and third parties should be in place. Contractual conditions may form part of these measures.

ABBREVIATIONS

Abbreviation	Description
CAF	Cyber Assessment Framework
CDOIF	Chemical and Downstream Oil Industries Forum
CMS	Competency Management System
COMAH	Control of Major Accident Hazards
DDoS	Distributed Denial-of-Service
DMZ	Demilitarized Zone
EU	European Union
HSE	Health and Safety Executive
IACS	Industrial Automation and Control Systems
IT	Information Technology
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NCSC	National Cyber Security Centre
NIS	Network Information Systems
OECD	Organisation for Economic Cooperation and Development
OT	Operational Technology
PCI	Payment Card Information
PHI	Protected Health Information
PII	Personally Identifiable Information
SMT	Senior Management Team

USEFUL RESOURCES

Further information on cyber security can be found from the following resources:

National Cyber security Centre	https://www.ncsc.gov.uk/
Health and Safety Executive	http://www.hse.gov.uk/eci/cyber-security.htm
National Institute of Standards and Technology	https://www.nist.gov

REFERENCES

Further information relating to cyber security can be found in the following publications:

Reference	Description
BS EN 62443-3-2: 2018 (Draft)	Draft Security for industrial automation and control systems. Part 3-2: Security risk assessment and system design. Based on IEC 62443-3-2: 2017
BS IEC 62443-2-1: 2011	Industrial communication networks — Network and system security Part 2-1: Establishing an industrial automation and control system security program
BS IEC 61508 Part 1 (normative) 2010 edition	Functional safety of electrical/electronic/ programmable electronic safety-related systems. General requirements
BS IEC 61511 Part 1 (normative) 2016 edition	Functional safety. Safety instrumented systems for the process industry sector. Framework, definitions, system, hardware and application programming requirements
INDG277 (revision 1)	Leadership for the major hazard industries
ISO/TR 10013:2001	Guidelines for quality management system documentation
OG 86	Cyber security for Industrial Automation and Control Systems (IACS)
ISBN: 9780198295952	Volberda, H. W. (1998) 'Building the Flexible Firm – How to Remain Competitive'
HSG65	Managing for health and safety
NCSC	How cyber attacks work
NCSC	NCSC Board Toolkit
NCSC	Cyber security training for staff
NCSC	Cyber Assessment Framework
World Economic Forum	Advancing Cyber Resilience – Principles and Tools for Boards, January 2017
OECD	Types of Cyber Incidents and their losses
OECD	Corporate Governance
HM Government	UK Cyber security – The Role of Insurance in Mitgating and Managing the Risk
HSE	Inspecting Major Hazard Leadership and Investigating Leadership Failures in Major Accidents, COMAH Competent Authority, Operational Delivery Guide
HSE Competency Management	Managing competence for safety-related systems Part 1: Key guidance
HSE Competency Management	Managing competence for safety-related systems Part 2: Supplementary material
ORR Competency Management	Developing and maintaining staff competence, Office of Rail and Road, 2016
HSE Intelligent Customers	Human factors: Intelligent customer capability
HSE Intelligent Customers	Human factors: Key principles in contractorisation

Reference	Description
HSE Intelligent Customers	Using Contractors – A Brief Guide
bsi	PAS 1085:2018 - Manufacturing – Establishing and implementing a security-minded approach – Specification

ACKNOWLEDGEMENTS

This document was created as part of the Chemical and Downstream Oil Industries Forum Process Safety work stream.

CDOIF wish to record their appreciation to the working group members who were responsible for creating this guideline:

Name	Organisation
Peter Davidson (Chair)	Tank Storage Association
Andrew Dickinson	World Fuel Services
Callum Easton	Prosalus
Ian Alderson	Navigator Terminals
Linda Dixon	Local Fuel
Martin Morgan	P&I Design
Sarabjit Purewal, OBE	Health and Safety Executive
Robert Marshall	Health and Safety Executive
Graham Hipkin	Coryton Advanced Fuels
Andy Geddes	PX Ltd.
Edward Kessler	Engineering Equipment & Materials Users Association
Mike Nicholas	Environment Agency
Leighanne Moir	Scottish Environment Protection Agency

REVISION HISTORY

Rev.	Section	Description	Date	Changed By
0	All	First Issue for stakeholder review	30-Mar-2020	Peter Davidson
1	All	Stakeholder Comments incorporated	31-Oct-2020	Peter Davidson

APPENDIX 1 – CYBER SECURITY PERFORMANCE INDICATOR EXAMPLES

Provided for guidance only

1. **Total number of events**: Is this increasing or decreasing? Why? Assess the cost to value of the incidents detection, response and recovery processes, and look for patterns to identify key risks.
2. **Number of events per device or host**: Are there any devices or hosts which are more prone to security issues than others, causing increased risk? Why? Assess detection success rates and key risks per device or host.
3. **Time to detection**: How long is it taking your organisation to detect a security event? Are there ways to reduce this time?
4. **Time to resolution**: How long is your organisation taking to resolve an actual security event? Are there processes or technologies that can help you reduce this time? What are they? Assess your mitigation success and processes
5. **Cyber security Incidents & Responses**: The number of reported security incidents in a specific period and their implications. Tracking responses to these incidents and their success rate contributes to evaluating a security system effectively. Mean time to detect (MTTD) and Mean time to respond (MTTR) are valuable inputs to the security system performance metrics.
6. **Average Time and Cost to Scale**: The time to scale and resolve an incident, as well as the uptime and downtime during the incident, are key indicators of the performance of the deployed security system. This not only helps identify the time invested in resolving an incident, but it also helps track the loss of sales, revenue or production during the incident occurrence. The cost of cyber investigation, staff and resources employed in locating the incidents, data restoring, and malware removal are other key performance evaluators.
7. **Customer Impact Management**: Managing and dealing with the impact of a data breach on customers' systems.
8. **Technical Resource Competencies**: Current competency levels against competency requirements.
9. **Processes and Procedures:** all elements of the management system documented and in place to allow auditing to take place. The output of the management system audit.

Examples of the types of metrics that can be collated for the indicators above:

Examples of Process security metrics

- Number of un-planned procedural violations
- % of weak passwords (noncompliant)
- No. of unmitigated vulnerabilities and their severity

Examples of Network security metrics

- Successful/unsuccessful logons
- No. of incidents
- No. of viruses blocked
- No. of spam blocked
- No. of port probes

Examples of software security metrics

- Unnecessary software applications installed on OT systems
- Compliance with patching policy
- Compliance with update frequency of virus definitions
- Cost per defect

Other metrics may include:

- Number of incidents that were reported in the period especially if they lead to non-conformities
- Number of Malware attacks detected
- Outages as a result of attacks (ex: DDoS, ransomware, disgruntled employee)
- Lost or stolen corporate devices