High Value Manufacturing Catapult

Summer 2022

Five-step cyber security risk assessment for small and medium-sized companies in advanced manufacturing

Authors

The following centres were directly involved in the creation and assembly of the Cyber Security Risk Assessment for Advanced Manufacturing:

- University of Sheffield Advanced Manufacturing Research Centre – AMRC
  Lead author: Narcisa Pinzariu
- Nuclear Advanced Manufacturing Research Centre – NAMRC
  Contributors: Dimitrios Anagnostakis

Acknowledgments

The project team would like to express their gratitude to all the representatives from the following centres of the High Value Manufacturing Catapult for taking the time to read through the work presented herein and provide invaluable feedback for its improvement:

- Advanced Forming Research Centre – AFRC
- Centre for Process Innovation – CPI
- Manufacturing Technology Centre – MTC
- National Composites Centre – NCC
- Warwick Manufacturing Group - WMG

Terminology

APT	Advanced Persistent Threats
BPCS	Basic Process Control System
DCS	Distributed Control System
DoS	Denial of Service
HIPAA	Health Insurance Portability and Accountability Act
IACS	Industrial Automation Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OT	Operation Technology
PIPEDA	Personal Information Protection and Electronic Documents Act
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information & Event Management
SIS	Safety Instrumented System
TTP	Tactics, Techniques and Procedures
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

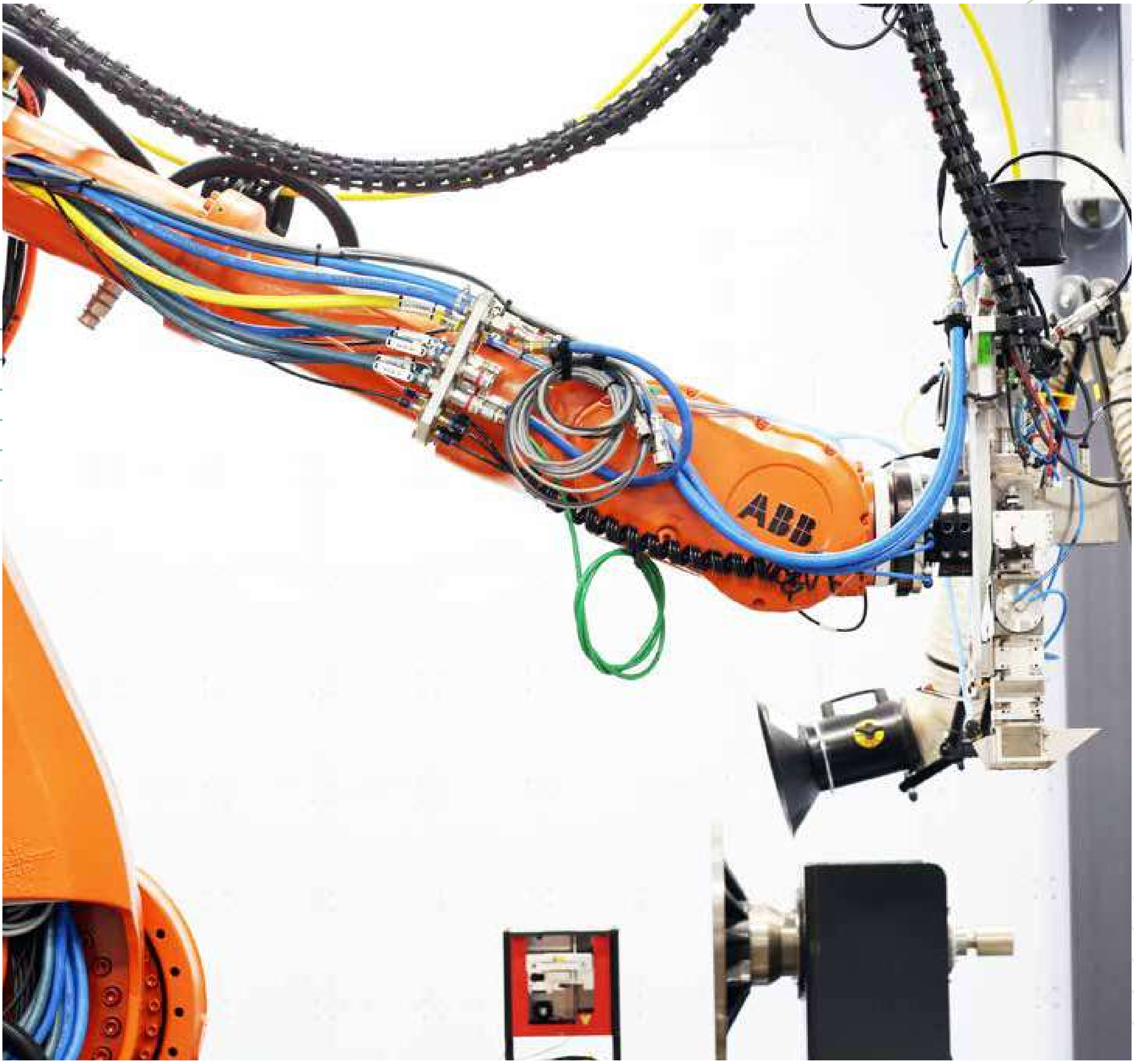
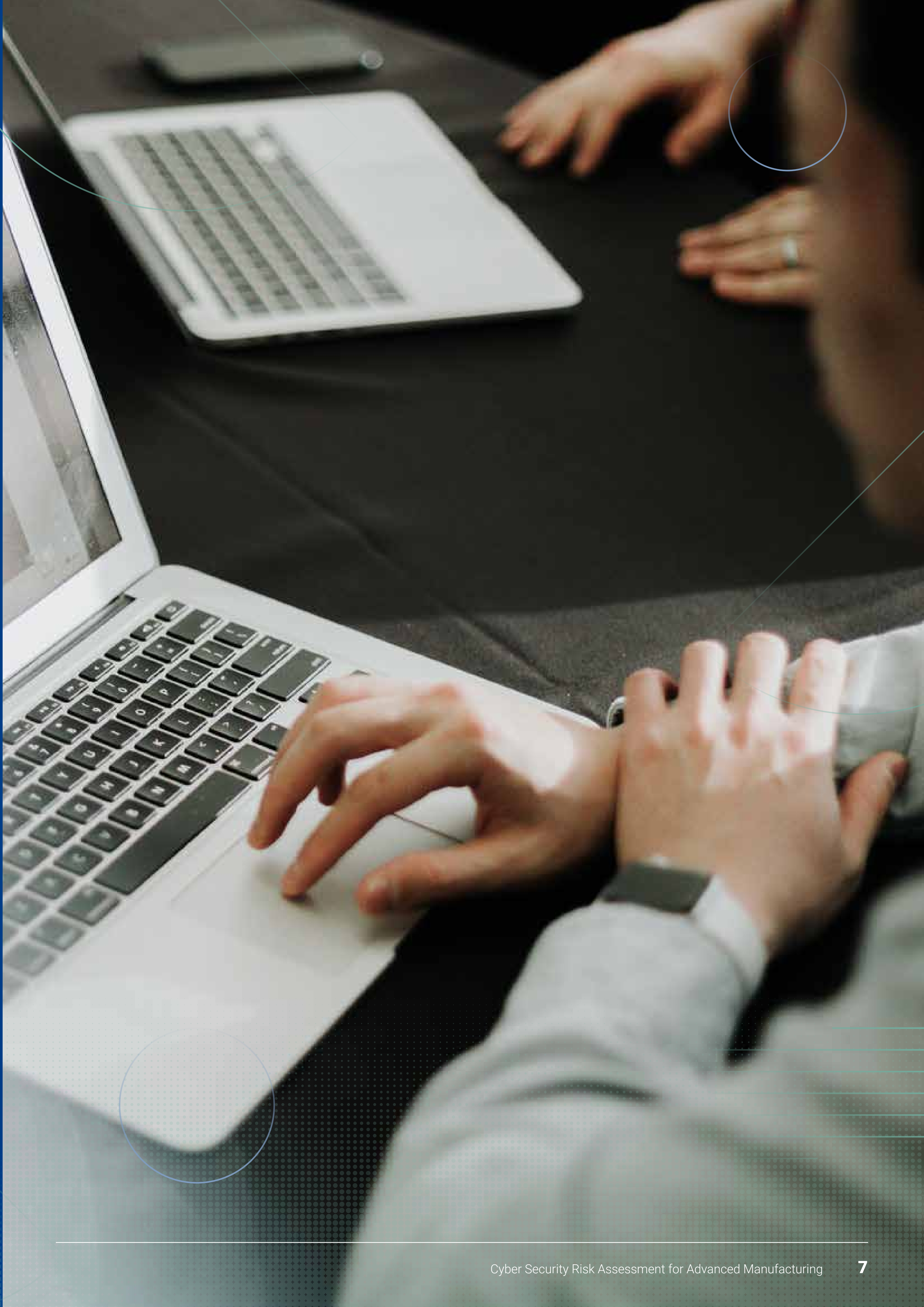


Table of contents

Table of contents (continued)

List of figures

List of tables



Introduction

The speed and scale with which manufacturers are embracing the growing benefits of technology, Industry 4.0 and the Internet of Things, are matched only by the potential for them to expose companies to accidental or malicious harm. Global connectivity and increased data sharing mean that a single unsuspecting click can put every site, customer, supplier and employee at risk. What's more, the company attacked may not even be the target, but simply a back door through which to access another business or individual.

During 2021, over a third of UK businesses (39%) were hit by a cyber-attack and a third of those (31) saw attempts made at least once a week, which of course does not include those that have quietly gone unnoticed. However, only 54% of business have assessed the risks in the last year, with just 43% having a cyber security insurance policy, 23% having a strategy and as few as 13% having considered the risk from their supply chain. With nearly half of businesses allowing employees to use their personal devices and the use of mobile technology for remote working (whether from home or travelling to different sites, customers or suppliers), it is worth noting that attackers capitalize on these options being less secure than corporate devices and site-based connectivity, which often have more effective protection.[i]

In advanced manufacturing, information and operating technologies make up a large percentage of a company's assets, with data at the heart of everything from machine centres and gateway devices to commercial and logistic networks. Effective cyber security keeps everything behaving as it should by maintaining confidentiality (data is protected), integrity (data is accurate and complete) and availability (data is ready to keep systems functioning, goods flowing and avoid expensive down time).

While large organisations are likely to have invested heavily in cyber security, many small and medium enterprises either don't have the resources to do so, don't believe they would be a target or don't find time to consider the risks because they are so focused on building the business and tackling other crises.

As emphasised throughout this guide, there is no single, simple or failsafe solution for cyber security, with both the operating environment and threats constantly changing. What's more, completing a cyber security assessment and developing the policies, strategy and mitigating actions to address the vulnerabilities it identifies is a lengthy and complex process, involving stakeholders from right across manufacturing, administrative and other functions. Yet to be truly effective, it shouldn't result in an unwieldy tomb that could prop open the factory gates. Instead, it should build into a living, breathing backbone that supports the overall business strategy by protecting current profits and future growth; a practical tool that is constantly used, discussed and updated, ensuring data driven decisions, design processes and manufacturing sites deliver as expected, while protecting the health, safety and legal rights of everyone involved.

This may seem daunting, which why this guide aims to help anyone creating, growing or managing a small or medium-sized company in the advanced manufacturing sector understand why cyber security poses a threat and what they can do about it. It provides a basic five-step framework for the risk analysis of operating technology to keep assets protected and working safely.

For those with little or no knowledge of cyber security, the guide offers a starting point from which to consider potential threats to their company, whether they can be tackled by existing in-house expertise, and, if not, how to frame any additional hiring or outsourcing. For those with some knowledge of cyber security, it offers a way to check they have considered the full breadth of implications for their business and identify any gaps that need addressing. And, while those with extensive experience will already be familiar with the contents, their feedback and case studies would be welcome contributions to help improve security across the entire sector.

> “ Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work – from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.
>
> **[NCSC 2021]**

Management Responsibility

Among boards or senior management within UK businesses[ii]:

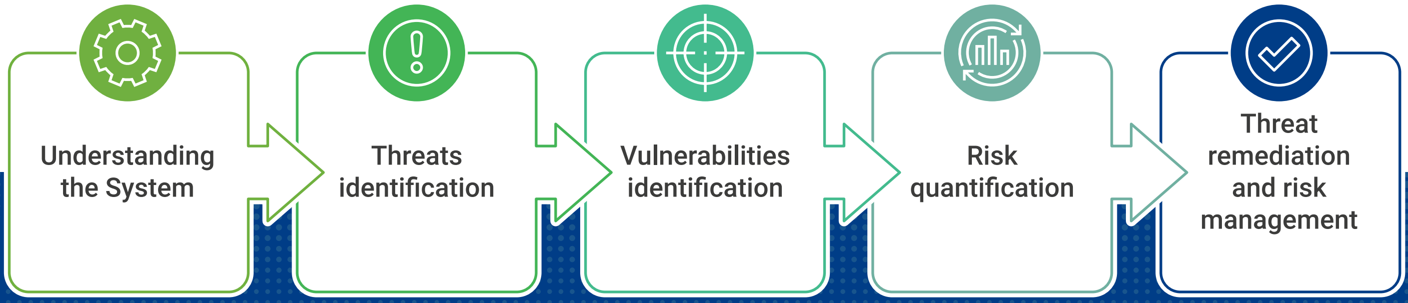
- 82% rate cyber security as a 'very high' or 'fairly high' priority.
- 50% receive updates on cyber security at least quarterly.
- 43% have an insurance policy that covers cyber-security.
- 39% use an external cyber-security provider.
- 36% have formal cyber security policies
- 21% working in utilities, production or manufacturing do not get cyber security updates.

Identified breaches or attacks

Among the 39% of UK businesses who report having a cyber security attack in the last year[iii]:

- Micro companies 36%
- Small companies 48%
- Medium companies 59%
- 21% were hit by denial of service, malware or ransomware.
- 31% were hit at least once a week.
- 83% were hit by phishing.

5-step Cyber Security Risk Assessment Framework



Understanding the System

Threats identification

Vulnerabilities identification

Risk quantification

Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

To ensure the risk assessment and recommended actions are aligned with the company's strategy and priorities, it is important to start by clarifying its scope and purpose in the context of existing policies and procedures around cybersecurity, budget planning and the overall appetite for risk, and to revisit those at each step.

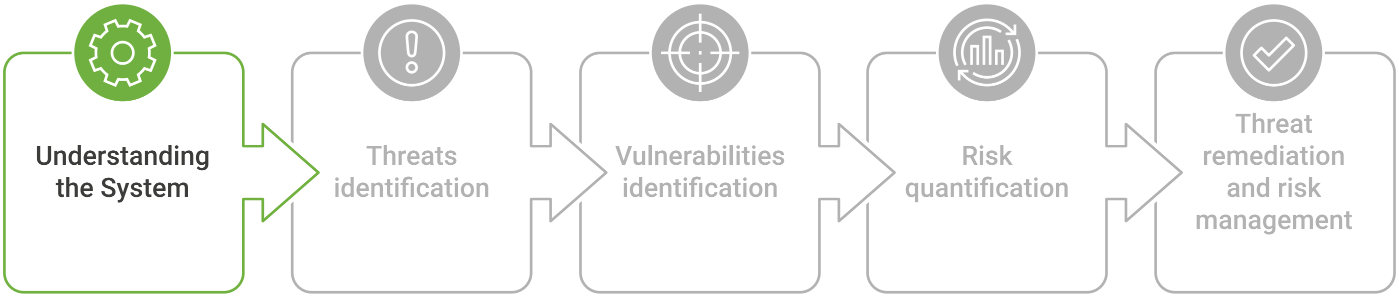
Cyber Security Strategy

Over a third (32%) of UK businesses have formal cyber security strategy[vi]:

- Micro companies 20%
- Small companies 37%
- Medium companies 48%

Within that, only 50% of micro/small companies and 65% of medium companies carried out a third-party review of their strategies.

1 Identify and understand the system



Understanding the System

Threats identification

Vulnerabilities identification

Risk quantification

Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

1.1 Identifying the system

The first step is to identify which system(s) and sub-units to assess, along with their security perimeter and access points, as each can have vulnerabilities that can be exposed and exploited for a cyber-attack.

Organisations normally have multiple control systems that should be considered for assessment, including all Industrial Automation Control Systems (IACS) assets, the components for which can be identified using from the organisation's system inventory, architecture diagrams, network diagrams and dataflows.

Some examples of components to include when identifying the systems for consideration are:

- Basic process control systems (BPCSs)
- Distributed control systems (DCSs)
- Safety instrumented systems (SISs)
- Supervisory control and data acquisition (SCADA)
- Industrial Automation Control Systems product supplier's packages
- Devices linked to the Internet of Things (IoT) and cloud-based solutions.

1.2 Defining the boundaries

Risk assessments can be carried out at three tiers of a business (Figure 1 below). It is advisable to focus on areas of the system that are of high value, offer a critical service, contain sensitive data and/or are most at risk of attack. Defining the boundaries in advance makes the assessment easier to complete, limits the length and identifies the necessary personnel.

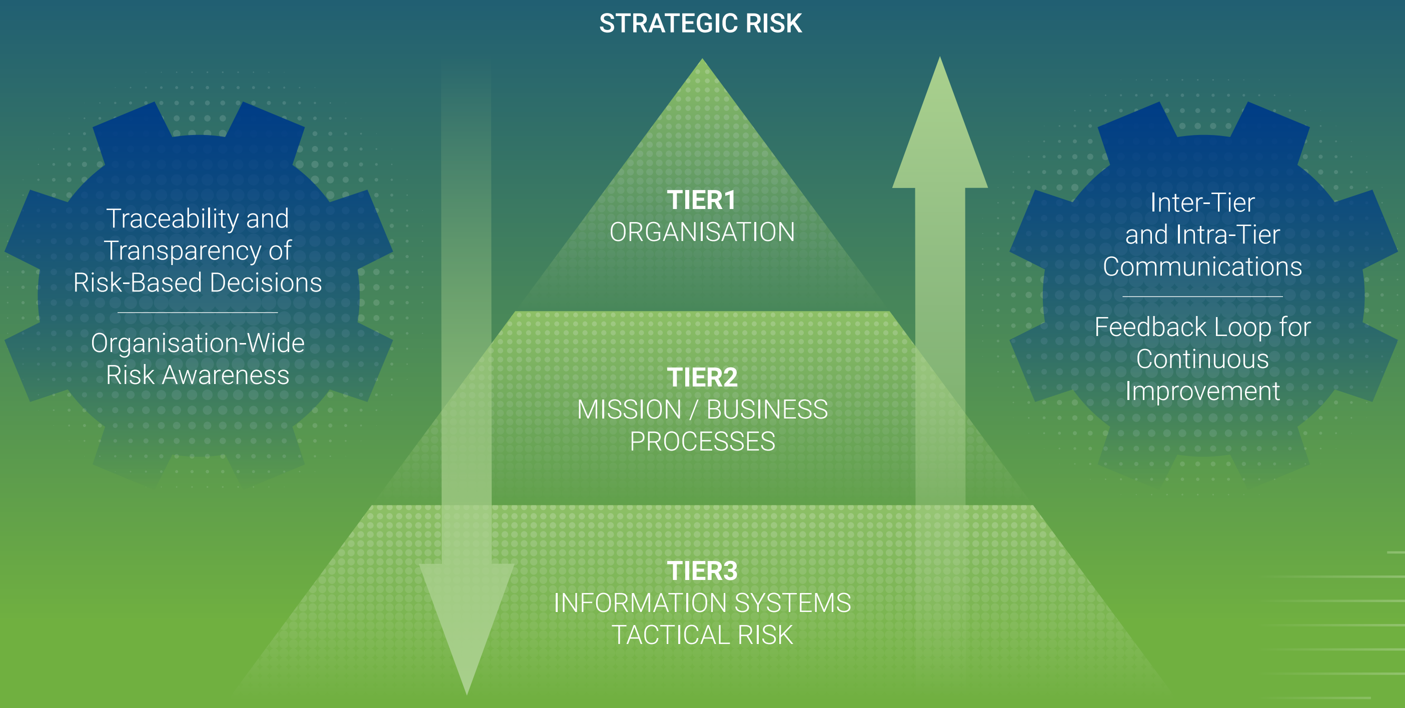

STRATEGIC RISK
Traceability and Transparency of Risk-Based Decisions
Organisation-Wide Risk Awareness
TIER1
ORGANISATION
TIER2
MISSION / BUSINESS PROCESSES
TIER3
INFORMATION SYSTEMS
TACTICAL RISK
Inter-Tier and Intra-Tier Communications
Feedback Loop for Continuous Improvement

Figure 1 Risk management hierarchy[vi]

Tier 1 – cyber security assessments can support company strategies, policies, programs, guidance and processes for managing risk, focusing on their operations, assets and individuals. This includes addressing the threats, weaknesses and/or deficiencies across multiple information systems, the adverse impacts caused by any loss or compromise of information, the use of new technologies and computing systems, and the potential impact on the company's ability to operate. It can affect decisions about cyber security, such as the type of risk response (tolerance, avoidance, mitigation, etc.), investment decisions, conformance with security architectures, and strategies for monitoring authorisation on systems and controls.

At Tier 2 – assessments can help to protect processes, operations and resilience requirements, as well as their alignment with an organisation's security architectures. They may also affect decisions about security architecture design, the selection of common controls, services and suppliers, the development of risk-aware processes and the interpretation of security policies for information systems and their operating environments.

At Tier 3 – assessments can again inform decisions about the selection and tailoring of security controls and systems, as well as those relating to their implementation (product and system configuration to meet security control requirements) and operation (monitoring, authorisations and maintenance). The assessment may include descriptions of vulnerabilities in the systems, along with risks and corrective actions, which can inform the organisation's overall risk evaluation while operating those systems and can feed back to Tiers 1 and 2.

As this suggests, cyber security assessments can also inform other risk management activities, both across and between the three tiers. For example, Tier 1 insights might feed into operational, financial, regulatory, reputational, supply chain and partnership risk management. At Tier 2 can provided similar insights for specific functions and operations, while Tier 3 can inform evaluations of cost, schedule and performance.

1.3 Discovering the assets

Having identified the systems for assessment and defined the boundaries, companies can focus on building an overview of the information, physical and human assets within them and the people responsible for them.

Common assets within a system include:

- Hardware, such as servers, network equipment, workstations, mobile devices etc.
- Purchased or bespoke software
- Information or data in any format (physical and/ or digital)
- Services provided to end-users (e.g. database systems, e-mail etc.)
- Locations and buildings (industrial and administration)
- Employees, temporary staff, contractors, trainees, volunteers, departing staff, etc.

The most common method for recording and managing this information is with an Asset Register and network and deployment diagrams, to which access should be carefully controlled through secure storage with password protection and encryption. This guide provides explains how to do this for Microsoft Office documents.

More information is available in Appendix 1, including what to include in an Asset Register, addressing assets or areas beyond the system owner's control, the lifecycle and obsolescence issues, registering secondary digital assets, and using diagrams to map the overall architecture of the system and its assets.

While 39% of UK business use an external provider, this varies significantly by size[vii]:

- Micro companies 35%
- Small companies 58%
- Medium companies 55%

1.4 Defining a system's current cyber security status

With the system and its assets identified, companies can determine their current security status and whether or not it meets their criteria for cyber security risk management.

Risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss caused by it (impact). Therefore, cyber risk is the probability of exposure or potential loss caused by an attack or data breach, given both the likelihood (vulnerabilities, exposure, threats, mitigating controls) and the impact (business criticality).

The system owner should identify existing cyber security procedures, then each asset owner should list them from least to most vulnerable to create a security posture rating. As a system's security posture rating increases, the cyber risk decreases.

The starting point is to map out what is known as the 'attack surface'. This is the set of interfacing points between a user and a piece of software or hardware, which an attacker could use to access or compromise an asset. It includes anything that could go wrong with devices, network infrastructure, apps, endpoints, Internet of Things, cloud, supply chains etc.

To generate an accurate picture of where the company has cyber-risks and ensure that risk mitigation efforts prioritize the highest risks, every point of the attack surface should evaluate:

- The severity of any vulnerability related to each asset.
- The threat level, given methods currently being exploited elsewhere by attackers.
- The risk of exposure from a vulnerability, depending on whether/how that vulnerability can be exploited and where/how the asset is deployed and used.
- The mitigating effects of any existing security controls.
- The business criticality of the asset.

1.5 Defining a system's baseline security criteria

According to the National Institute of Standards and Technology (NIST), a security control baseline refers to the "minimum security controls defined for a low-impact, moderate-impact, or high-impact information system"[viii]. Figure 2 shows how cyber risk tolerances impact technology use.

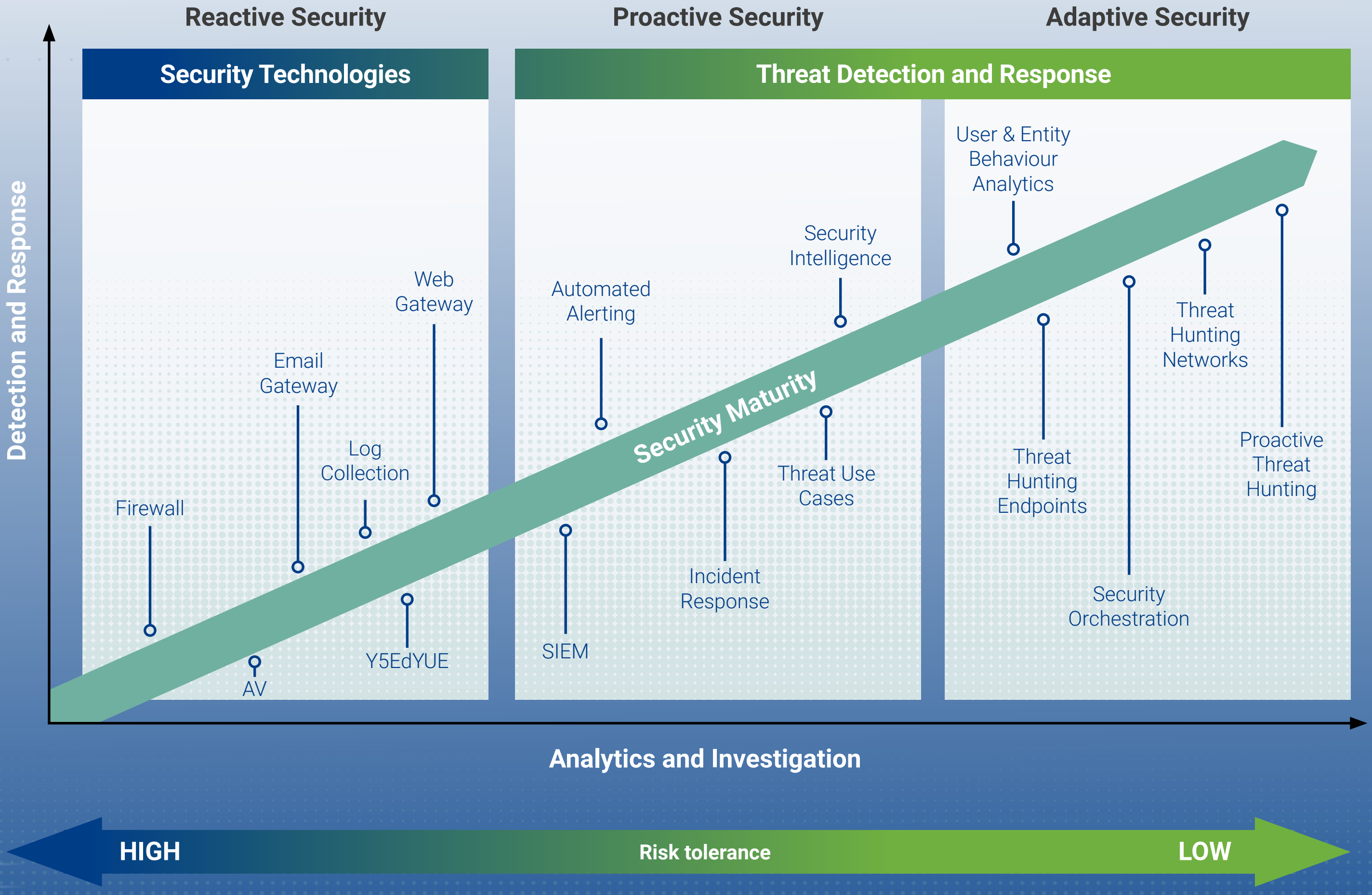


Figure 2 A perspective on how high and low cyber-risk tolerances impact technology use[ix]

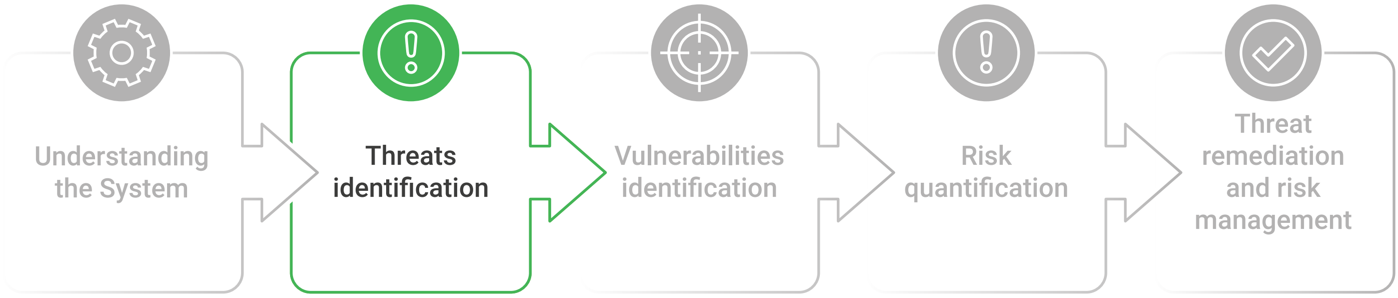
Before defining baseline security criteria, the company must define the level of risk it is willing to assume by identifying which of their assets are critical (either because of their function or how they interact with sensitive data) and where they are located. This should take account of factors such as compliance drivers, security threats, data and asset value, industry and competitive pressure, and management preferences, as shown in Table 1 below.

Table 1 Factors to consider when defining the risk tolerance

Risk tolerance level	Factors
High	No compliance requirements
	No sensitive data
	Customers do not expect your organisation to implement and maintain strong security controls.
	Innovation and revenue generation comes before security, so more risk is accepted.
	Organisation does not have remote locations.
Medium	Some compliance requirements (e.g. HIPAA, PIPEDA).
	Some sensitive data, required to retain records.
	Customers will eventually need strong security controls for their activities.
	Due to the sensitive data, information security is more visible to senior management.
	Organisation has some remote locations.
Low	Multiple compliance requirements and house sensitive data, e.g. medical records.
	Customers require and expect your organisation to have and maintain strong security controls.
	Information security is highly visible to senior management and public investors.
	Organisation has multiple remote locations.
	Assess the security pressure posture

> Before defining baseline security criteria, the company must define the level of risk it is willing to assume by identifying which of their assets are critical...and where they are located.

2 Threat identification


Understanding the System

Threats identification

Vulnerabilities identification

Risk quantification

Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

A cyber security threat is any circumstance or event that could adversely impact a company's operations, assets, employees, reputation or other organisations with which it works. This can be through unauthorised access, destruction, disclosure, or modification of information, and/or denial of service, whether intentional or not. For manufacturers, such a threat can impact their ability to maintain at least one of the following.

- **Confidentiality** (data is protected). Attackers can access, manipulate or steal data about industrial processes, configurations, intellectual property, and corporate or product information. They can do this using passive analysis of network traffic, injecting code to obtain security credentials or corrupting control measurements.
- **Integrity** (data is accurate and complete). Sabotage can alter or delay network traffic or industrial communication protocols, many of which link to legacy assets predating current security considerations. Such vulnerabilities can attract Advanced Persistent Threats (APT), where attackers infiltrate a network for as long as possible, while modifying the system's function, collecting data or gaining access to more devices.
- **Availability** (data is ready to keep systems functioning, goods flowing and avoid down time). Attackers can make a system unavailable by overloading it, either through the machinery or network access. A distributed denial of service (DDoS) is a common attack that has increased with cloud computing and can either flood the bandwidth with requests, pass malformed data to crash a process, or use a virus to destroy or disable a sensor.
- **Authentication** (data access is controlled by verifying the user). Attacks often use phishing or spam email chains that target design flaws, misconfiguration and software or user vulnerabilities to escalate privileges and gain access to strategic information, protected data or other resources, whether physical or digital.

Since most factory and office devices are connected, a single vulnerability can be critical for the entire business. This means a lack of awareness or training can turn a dedicated employee into an accidental threat if they plug in an unsafe USB memory stick, access a process control zone with an infected laptop, or compromise their security credentials by inadvertently opening a phishing email. With collaborative networks, cloud technology and the Internet of Things, that can quickly become a threat to the entire network of customers, suppliers and partners.

2.1 Identification of threat sources

A threat source can be a person, action or situation that either accidentally triggers or intentionally exploits vulnerability. These can include hostile cyber or physical attacks; human errors of omission or commission; structural failures of organisation-controlled resources (e.g., hardware, software, environmental controls); natural and man-made disasters, accidents, and failures beyond the control of the organisation.

A company may identify multiple internal and external sources for a potential cyber threat, but they won't always turn into an attack or an incident. Work to identify them, should take account of:

- The scope and relevance for the company.
- Layers affected, including for execution (sensors, actuator), data transport (network), applications (data storage).
- The capability, intent and target of potentially malicious sources.

The International Electrotechnical Commission 62443 framework, which is the standard for industrial cyber security recommends documenting the source, its capability and possible vectors and assets that could be affected. .

▶ Appendix 2A provides more information to help collect and document threat sources

2.2 Identification of threat events

The likelihood that a threat event will actually occur is assessed with respect to:

- A specific time frame (e.g., the next six months, year, or a specified milestone) and estimated frequency of any events almost certain to occur.
- The state of the company and vulnerabilities/predisposed conditions, including core processes, enterprise and information security architecture, information systems, operating environment and existing safeguards.

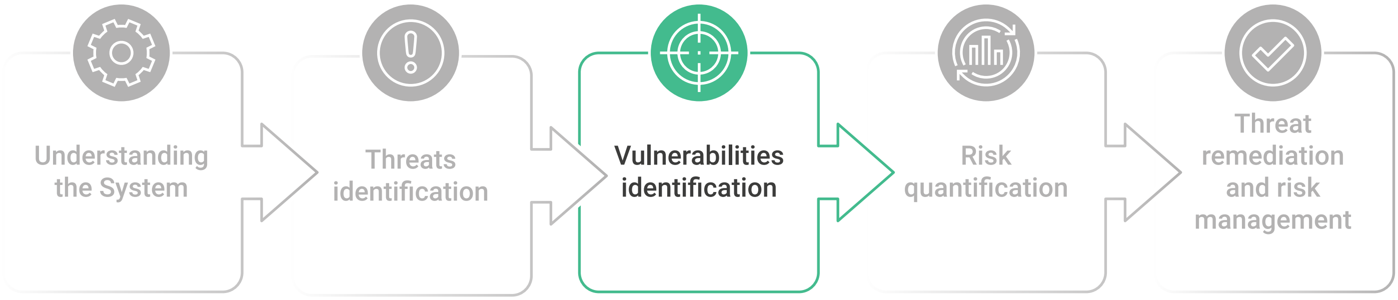
Regardless of the magnitude of harm, companies should assess the probability that the threat event will have an adverse impact and quantify its relevance against their risk tolerance. This includes considering whether the threat events will be initiated (adversarial/malicious/deliberate) or will occur (non-adversarial/unintentional/accidental) and their operations, assets, individuals or other organisations.

A single threat source can initiate multiple events. For example, a phishing email allowing access to data and infecting other networks for long periods without being detected. Likewise, multiple threat sources can initiate or cause the same threat event. For example, a server can be taken off-line by a denial-of-service attack, a deliberate act by a malicious system administrator, an administrative error, a hardware fault, or a power failure.

This makes it extremely complex, but equally important, for manufacturing companies to accurately identify, document and map the relationships between events and their sources, while addressing both adversarial and non-adversarial events, as well as their impact on operations, assets, individuals or broader industrial networks.

▶ Appendix 2B provides more information and sample tables to help document and evaluate threat events

3 Vulnerabilities identification



Understanding the System

Threats identification

Vulnerabilities identification

Risk quantification

Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

Vulnerabilities in the system, security procedures, internal controls, or implementation that can be exploited by a threat source should be identified and addressed to prevent or mitigate the impact, along with any predisposing conditions that could influence that outcome.

Most system vulnerabilities can be associated with security controls that have weaknesses or have not been applied, whether intentionally or not. Similarly, a smart manufacturing system might have vulnerabilities due to the complexity of connections between the equipment within a system, remote access to them and/or issues with software, hardware and local or wireless networks. What's more, new vulnerabilities can emerge as a manufacturer, its operating environments and technologies evolve, reinforcing the need for continual monitoring and risk assessments during the entire life cycle of a system.

Vulnerabilities related to some predisposed conditions are easy to assess, such as facilities in flood zones or systems with no external connections, while others are more complex, such as gaps in contingency plans, outdated technologies or system backup deficiencies. However, as they impact the company's security posture and the likelihood of a threat event, the severity of all vulnerabilities and persuasiveness of predisposing conditions should be considered for the three tiers mentioned in Figure 1 above.

▶ Tables to help are provided in Appendix 3A.

Outdated software

Companies still use older, unsupported versions of Microsoft Windows (pre-8.1), which are more vulnerable to a security threat[x]:

- Micro companies 16%
- Small companies 20%
- Medium companies 25%

There are three common techniques to help identify and monitor vulnerabilities.

3.1 Gap Assessment

This identifies and quantifies the differences between the current and target states of a system, and the actions required to reduce them, by using employee interviews, site tours, and reviews of policies, processes and technologies. Industry standards that can support this process are supplied in Appendix 3B.

3.2 Penetration Testing

This attempts to breach some or all of the system's security, using tools and techniques an adversary might employ. This approach is suitable for identifying vulnerabilities and risks on an operational system with components and services from multiple vendors, and for systems and applications developed in-house. However, it is not appropriate for product specific testing and can only validate security on known issues on the day of the test, whereas vulnerabilities can exist for long periods. There are several types of test.

a) Vulnerability identification in bespoke or niche software. This is usually carried out in web applications and provides feedback on coding practices that avoid introducing the categories of vulnerability identified.

b) Testing different scenarios to check if any lead to a vulnerability. This may include a lost laptop, unauthorised device connected to internal network, compromised host and many others.

c) Testing different scenarios to check the company's ability to detect and respond to vulnerabilities. The effectiveness is limited to the specific scenario on each test.

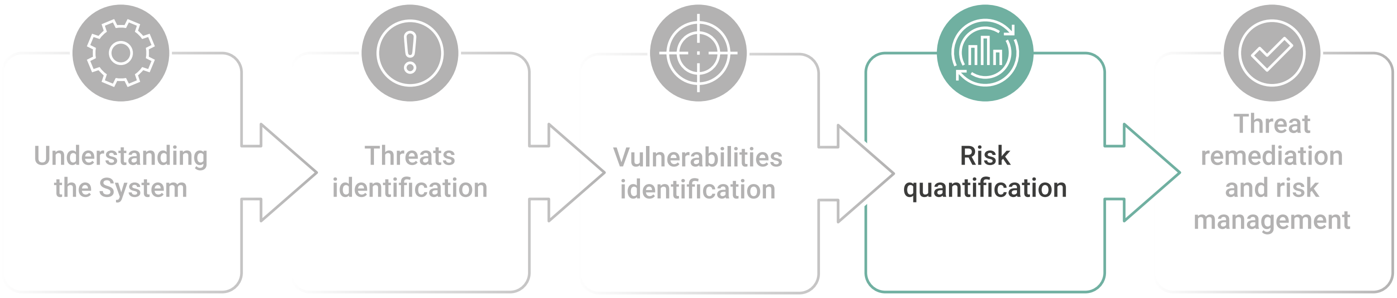
Each of these can be carried out with or without giving testers information about the system in advance.

- White-box testing: full information is supplied to check if the assessment and controls were effective by identifying software issues, vulnerabilities and misconfigurations.
- Black-box testing: no information is supplied to check if or how a system or asset can be attacked by discovering any previously unidentified vulnerabilities.

3.3 Active & Passive Testing

An active assessment scans the network to find devices, software or firmware versions and any potential vulnerabilities they create, with the aim of placing traffic that could introduce risk and detect the outcomes. A passive assessment discovers network devices using means such as surveys, architecture drawings, system logs, equipment configuration files, traffic analysis.

4 Risk quantification


Understanding the System
Threats identification
Vulnerabilities identification
Risk quantification
Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

The risk quantification is done in three main phases, which are illustrated by tables provided in Appendix 4.

4.1 Determine likelihood threats will occur or vulnerabilities be exposed.

The likelihood is a weighted risk factor based on the probability of a threat source actually exploiting vulnerabilities and can be broken down into categories to improve accuracy. This can be assessed qualitatively or quantitatively.

4.2 Determine the severity of the impacts on the company or system if a threat event occurs.

The scale of severity affects how the company will prevent the event or mitigate the consequences. Again, this can be broken down into categories, with multiple options for classification.

4.3 Calculate the overall risk.

Risk matrices are used to determine the level of a risk considering the likelihood of an incident occurring and the severity of the impact if it does, which informs decisions about control measures and mitigation plans.

As the objective is to preserve the confidentiality, integrity and availability of the assets within a manufacturing environment, a deeper investigation could link each of those elements to the threat or vulnerability being assessed.

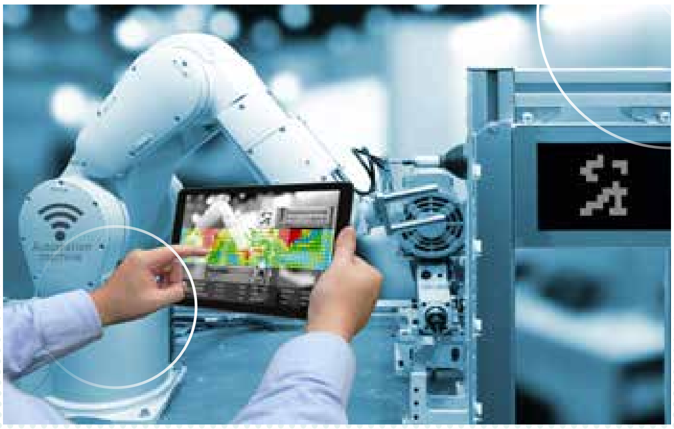
This can start to feed into the creation of a Risk Register, which collates and stores all the information for easy reference, and a management strategy, which takes account of issues such as the costs of deploying a preventative measure and the value of the company's reputation.

Risk quantification

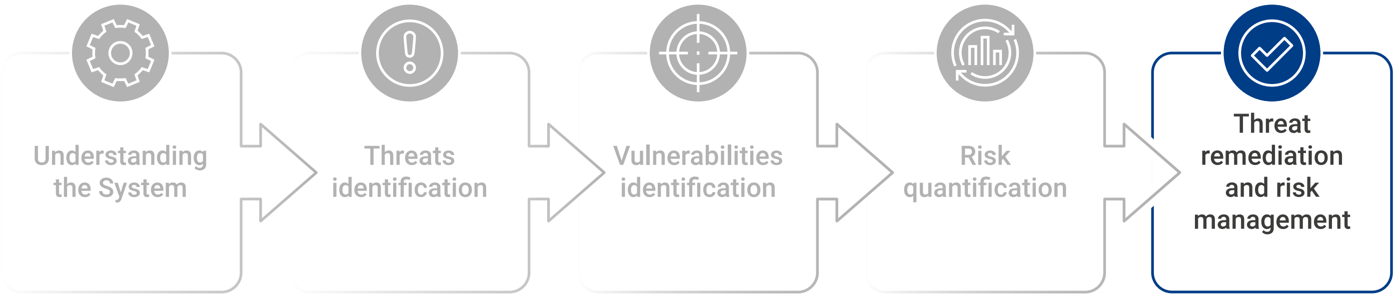
Among UK businesses, in the last year[xi]:

- 54% took action to identify cyber-security risks
- 33% conducted a risk assessment

▶ Appendix 4 includes a sample Risk Register.



5 Threat remediation and risk management


Understanding the System

Threats identification

Vulnerabilities identification

Risk quantification

Threat remediation and risk management

1.1 Identify threat sources
1.2 Setting the boundaries
1.3 Asset discovery
1.4 Current status
1.5 Baseline criteria

2.1 Identify threat sources
2.2 Identify threat events

3.1 Identify vulnerabilities
3.2 Predisposing conditions

4.1 Determine likelihood
4.2 Determine severity
4.3 Calculate risk

5.1 Preventive measures and security practices
5.2 Technical controls and countermeasures

5.1 General preventative measures and security practices

Although system risks and vulnerabilities cannot be completely eliminated, remediation and management can reduce how accessible they are or how much impact they will have. These measures do not necessarily consider the specifics of a system, but will still help to mitigate any risks a system may have. When implementing preventative measures and security practices, the following points should be considered.

5.1.1 Risk review

The company must first consider the threat landscape (Section 2 above) and which risks are acceptable or not, taking account of whether or not they would affect[xii]:

- mission-critical business systems (internal or external).
- health, safety and well-being.
- databases containing sensitive information.
- core infrastructure and partner portals.
- legal and contractual requirements.

It should also consider how often to review the risks, the appetite for one or more of them, and the need to mitigate them depending on its size, resources, assets and devices, amount and type of data. Even if a risk is considered acceptable, it must be systematically monitored to ensure it doesn't increase and the mitigating actions remain valid, including evaluating against previous risk assessments and the Risk Register.

5.1.2 Training

Some threat events are accidental and can originate from within the company. Cyber security awareness and training should ensure that all new and existing employees understand the policies (eg. using personal devices), responsibilities (eg reporting incidents) and threats (eg malware or phishing).

This means regularly monitoring levels of awareness, skill and training among technical, non-technical, privileged and executive roles, depending on whether they are directly or indirectly associated with critical system, assets or data, and on the resources available. The aim should be to create a culture where everyone not only follows rules for cyber security, but also takes ownership and feels empowered to voice concerns without fear of reprisals.

Using Personal Devices

Only 17% of UK businesses carried out staff training in the last year, yet nearly half (45%) allow staff to regularly use personal devices for work[xiii]:

- Micro companies 46%
- Small companies 42%ed
- Medium companies 43%

5.1.3 Passwords & access control

Passwords are simple, low-cost security measures, which offer the first line of defence against malicious attacks and are used in many assets (often set by the manufacturer during production). However, passwords can be obtained in many ways including phishing attacks, data breaches, brute-force attacks, employees keeping notes or being left unchanged from the default setting. As indicated earlier, once an attack breaches a single vulnerable point in a company, it becomes much easier to access and damage multiple systems, assets, devices and databases.

Below are some of the simple steps that can improve password security[xiv]:

- Reinforcing a password with multi-factor authentication (MFA), which only lets the user gain access by verifying a second element such as a code sent by text/email, a third-party app for smartphones or biometrics.
- Providing password management software (protected by a master password and MFA) to help users track and remember passwords for different accounts. However, an attacker accessing this, could access all passwords.
- Monitoring and limiting the number of logins attempted before the user is obliged to contact their system administrator and prove their identity.
- Maintaining a database of unacceptable or commonly used passwords, which users are prevented from adopting when they create or change an account.
- Setting password standards, such as a minimum number/combination of characters, letters numbers and symbols, or passphrases (string of dictionary words), which can be hard to crack and guess.
- Changing default passwords for software and hardware on delivery or as soon as possible thereafter.

In addition to passwords, secure access to any information/services within systems and physical premises, should be controlled by registering users and only providing the rights necessary to perform their specific role. Such access should be regularly controlled by asset owners, particularly when someone leaves or joins the company.

> “..passwords can be obtained in many ways including phishing attacks, data breaches, brute-force attacks, employees keeping notes or being left unchanged from the default setting.

5.1.4 Patch management

When a vendor identifies a vulnerability in their product that can't be directly fixed by the user, they can issue patches to update the software or device to prevent attackers from exploiting it. Regular checks should be carried out by personnel who can easily identify and prioritise areas of exposure and risk in the system, then immediately launch mitigating controls and contact the vendor to check if there is a patch.

However, each patch only addresses a specific vulnerability and does not make a solution completely secure .

Patches should only be obtained from reputable sources, ideally the Original Equipment Manufacturers (OEM), and should be tested before deployment, using a predetermined methodical approach, which should include:

- Backing-up the system, components, data, configuration, bespoke programs and code before starting.
- Establishing testing procedures to ensure the patch fixes the vulnerability without introducing new issues.
- Identifying critical systems/assets that will be affected and a priority order to determine which to patch first.
- Considering if a component is still required in a system, if another approach should be used or if the component should be removed entirely before patching it.

An OEM will usually publish a vulnerability report on their website detailing the issue, the products affected and mitigating actions to prevent exploitation while a patch is being produced. If a company finds a vulnerability not yet listed, it may be a new discovery and should be reported to the OEM. The company should stay up to date, for example with alerts section of the CISA website, NIST for vulnerability disclosures and/or NCSC weekly reports

5.1.5 System partitioning & segmentation

This groups assets into zones or conduits based on factors such as risk, criticality, function, physical/logical location, required access and/or the responsible party[xvi]. For example, a manufacturing environment and its system could be divided by operation (eg material storage, treatment, processing) and by function (eg layers of automation).

The aim is to group assets with common security requirements, making it easier to apply mitigation measures (eg firewalls) to the connection of each zone or conduit, with conduits grouping assets dedicated to communication. This segmentation approach also means that should a zone or conduit be infected with malware or other malicious code, it will be contained the threat instead of allowing it spread through the whole system.

Partitioning and segmentation are best applied during the design and implementation of a system. Applying them retroactively to a system will be more expensive, take longer and create down-time, but will still reduce the risks.

Appendix 5A illustrates how this approach should (and should not) be implemented.

Cyber security controls

Almost every UK business has at least one rule or control in place[xvii]:

- Data back-ups (87%)
- Malware protection (83%)
- Password policies (75%),
- Network firewalls (74%)
- Restricted IT administration rights (72%)
- Secure cloud service data backup (71%)
- Two-factor authentication (37%)*
- Monitoring user activity (33%)
- Providing separate Wi-Fi for staff and visitors (33%)
- Using virtual private networks (32%)

5.2 Technical controls and countermeasures

The general preventative measures and security practices above, are normally combined with technical controls and countermeasures that prevent and monitor malicious content within a system/network.

5.2.1 Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

These monitor and protect networks by helping to block, copy and analyse malicious content. Although used in tandem, many IDS or IPS solutions include both, so you only need to purchase one.

IDS passively monitor network traffic by copying and analysing the signature of packets coming over the network, then notifying the user of malicious packets so they can identify where they came from and what they contained. This can identify malicious content without affecting the packets, but can't do anything to prevent them. Some examples of IDS include SolarWinds Security Event Manager, Kismet, Zeek, Open DLP, Sagan, and Suricata.[xviii]

IPS actively monitor the network traffic, but unlike IDS, can block malicious content by analysing the packets' headers and payloads. However, they can't prevent future malicious content. Some examples of IDS include SolarWinds Security Event Manager, Datadog Real-time Threat Monitoring, Zeek, Splunk, Sagan, and Fail2Ban.[xix]

5.2.2 Security Information & Event Management (SIEM)

These solutions can monitor, find and stop threats immediately by analysing data in real-time. They can provide forensic capabilities by capturing, aggregating, storing, investigating and reporting log data from security devices/solutions, network infrastructure, systems and applications. This can be combined with contextual data about users, assets, threats, providing an overview to identify risks, vulnerabilities and ways to mitigate them.[xx]

SIEM solutions, such as Arcsight ESM, IBM QRadar and Splunk[xxi xxii], can be used in many scenarios, such as:

- Addressing and managing both potential and successful breaches to limit damage and recovery time.
- Monitoring user activity, privileges and security compliance to pinpoint breaches.
- Recognising abnormal activity, assessing the risk and prioritising the response.
- Using advanced analytics to gain insights from collected data.

5.2.3 Firewalls

Whether software or hardware, firewalls provide a buffer between networks within the company and/or elsewhere (eg the internet) by filtering network traffic to decide if it should be allowed in, out or blocked.

5.2.4 Malware & antivirus protection

Malware codes are usually downloaded via a malicious email file, mobile device or website, then spread among other devices on the same network, creating vulnerabilities and/or stealing, editing, encrypting or deleting data. Most operating systems have basic built-in antivirus protection, but it is much better to install third-party software.

5.3 Mitigation strategies & defence in depth

A robust mitigation strategy should combine the measures in this section with some of those in Appendix 5B, depending on the likelihood, severity and acceptability of each vulnerability and risk. For example, a 'defence in depth' strategy integrates multiple solutions for different assets and risks related to people, technology and operation capabilities, establishing variable barriers across the company/ system.[xxiii] This makes a breach more expensive to do and more likely to be detected, while ensuring the company is more capable of dealing with it.

5.4 Residual risk & acceptable risk

As no system can be completely secure, after the above mitigation measures are applied, any residual risk should also be identified, evaluated against the overall risk review and included in the Risk Register, following the same steps as earlier. This lets the company monitor and measure the effectiveness of those original measures and to determine if any residual risks represent an acceptable level of loss/disruption for a specific system.[xxiv]

5.5 Incident response and recovery plan

Every company should have a response and recovery plan, which reduces or prevents the loss of data/system downtime, enables them to investigate any incident and allows data/systems to be restored as quickly as possible. All employees should be aware of the plan, how the decisions are coordinated and their responsibilities within it.

> “Every company should have a response and recovery plan, which reduces or prevents the loss of data/system.

Appendices

Appendix 1 - Asset discovery

Before starting, it is important to define procedures and responsibilities for identifying, recording and managing the assets of the system to be evaluated. This includes creating an Asset Register with the following information:

- Unique identifier, location and zone reference
- Asset / conduit type, manufacturer, serial number etc.
- Risk profile/criticality information (e.g. risk-level, restore criticality, Common Vulnerability and Exposures etc.)
- Responsible person (where responsibilities are divided, e.g. between different departments)
- Network connectivity arrangements (e.g. addresses, ports, connection type, network protocols, encryption algorithms etc.) for each network connection.
- Network connection type, e.g. for multi-homed assets, or other (e.g. fieldbus) connections.
- Conduits – expected data flows to allow data flow rules to be defined.
- Any temporary connections such as portable assets (e.g. laptops) and assets where portable media connections are required / used.
- Firmware, operating system, and application software (including security software such as AV) types and versions (could be part of another system rather than the asset register but should be recorded).

The system owner should also identify assets or parts of the system that they have no control over. This can include products or services that may collect information about the system or its users, and are provided by a third party or vendor. Here the user has control over whether they use the asset within the system and to a lesser extent how the asset is used within the system but has no control over how the asset functions.

The procedures for managing assets should include decision making processes, plans or roadmaps for what happens throughout their lifecycle, in particular, when they become obsolescent. It is also important to recognise that industrial assets tend to have much longer operational lifespans than commercial IT systems.

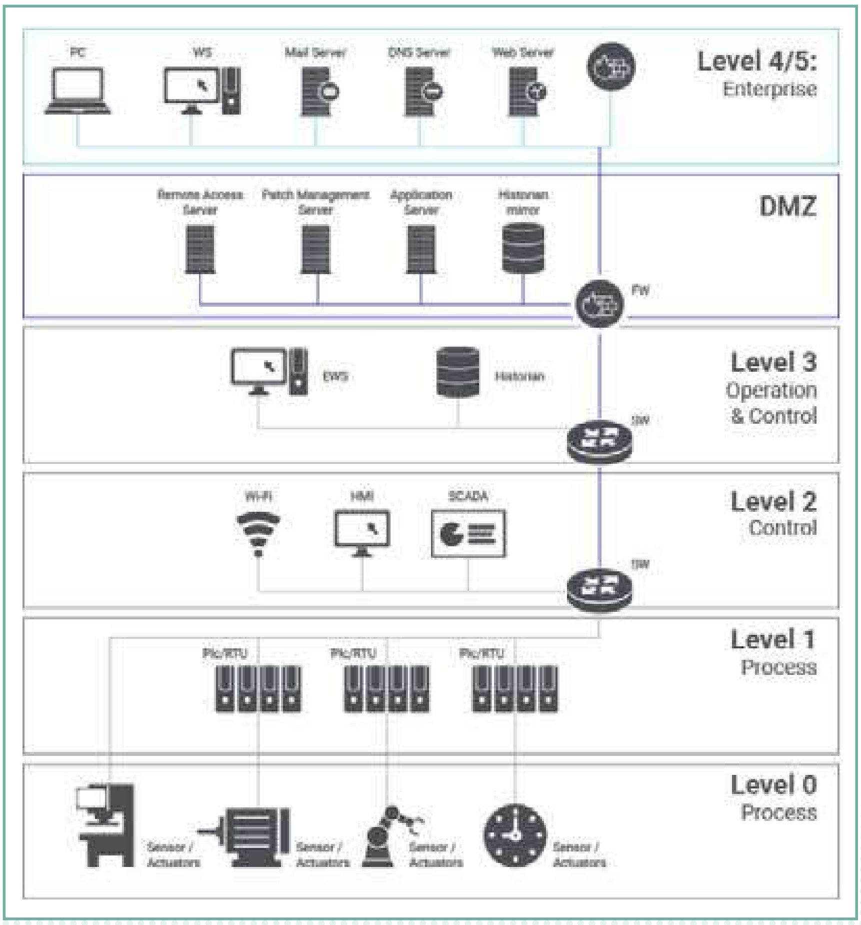
If a system has many assets or applications, it may be useful to create a secondary digital asset list, which includes:

- Software name and publisher
- Installation date, version number and motivations
- Local and remote roles
- Generic accounts
- Dedicated accounts
- Access control list with read, write and execution rights
- When existing, outgoing connections shall be considered (IP/Ports destination). If unknown, information shall be identified as “missing”
- Licence number.

Diagrams are important in understanding the system. They should show the architecture and topology of the system, and how the elements of the Asset Register are connected, including:

- List of Internet Protocol (IP) address range with, for each one:
  - The list of switches concerned
  - The functional description of the IP range;
  - Interconnections with other ranges.
- List of non-IP networks with, for each network:
  - The list of Media Access Control (MAC) addresses or addresses specific to the industrial protocols on the network
  - The list of switches concerned
  - Functional description of the network
  - Devices connected to the other network (connectors).
- List of non-Ethernet access points with, for each one:
  - The list of access ports
  - Addressing, if there is a special protocol
  - The list of connected devices.
- List of logical servers and desktops with, for each one, if applicable:
  - IP addressing (network, mask, gateway)
  - Operating system version
  - Underlying physical server
  - Applications and their versions
  - Services and versions
- List of connectors and communication field devices (remote input/output, smart sensors, smart actuators, etc.) with, for each one:
  - IP addressing (network, mask, gateway) for associated MAC addressing and network or the specific addressing, if appropriate
  - applications
- Interconnection points with "external" entities and all interconnections with the internet.

Figure 3 The Purdue model - a structural model for industrial control system (ICS) security, concerning physical processes, sensors, supervisory controls, operations and logistics. (Source: Zscaler)



Appendix 2A - Threats sources identification

Table 2 Possible inputs to threat source identification task (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organisation level) ■ Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). ■ Threat source information and guidance specific to Tier 1 (e.g., threats related to organisational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). ■ Taxonomy of threat sources, annotated by the organisation, if necessary. ■ Characterization of adversarial and non-adversarial threat sources. ■ Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organisation, if necessary. ■ Assessment scale for assessing the range of effects, annotated by the organisation, if necessary. ■ Threat sources identified in previous risk assessments, if appropriate.	No	Yes	Yes if not provided by Tier 2
From Tier 2: (Mission/business process level) ■ Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). ■ Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via peer sharing	Yes
From Tier 3: (Information system level) ■ Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). ■ Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via RAR	Yes via peer sharing

Table 3 Taxonomy of threat sources (National Institute of Standards and Technology, 2012)

Type of Threat Source	Description	Characteristics
ADVERSARIAL ■ Individual - Outsider - Insider - Trusted Insider - Privileged Insider ■ Group - Ad hoc - Established ■ Organisation - Competitor - Supplier - Partner - Customer ■ Nation-State	Individuals, groups, organisations, or states that seek to exploit the organisation's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting
ACCIDENTAL ■ User ■ Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
STRUCTURAL ■ Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller ■ Environmental Controls - Temperature/Humidity Controls - Power Supply ■ Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL ■ Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun ■ Unusual Natural Event (e.g., sunspots) ■ Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organisation depends, but which are outside the control of the organisation. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Table 4 Threat sources identification and assessment - characteristics of adversary capabilities (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table 5 Threat sources identification and assessment - characteristics of adversary intent (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organisation’s information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organisation’s information systems or infrastructure. The adversary is very concerned about minimizing attack detection/ disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organisation’s cyber resources by establishing a foothold in the organisation’s information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organisation’s missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/ disrupt the organisation’s cyber resources and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organisation’s cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

Table 6 Threat sources identification and assessment - characteristics of adversary targeting (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyses information obtained via reconnaissance and attacks to target persistently a specific organisation, enterprise, program, mission or business function, focusing on specific high- value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organisations.
High	80-95	8	The adversary analyses information obtained via reconnaissance to target persistently a specific organisation, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyses publicly available information to target persistently specific high-value organisations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organisations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organisations or classes of organisations.

Table 7 Threat sources identification - range of effects for non-adversarial sources

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are **minimal**, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], and involving no critical resources.

Appendix 2B - Threats events identification

Table 8 Possible inputs for the threat identification task (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organisation level) ■ Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). ■ Threat event information and guidance specific to Tier 1 (e.g., threats related to organisational governance, core missions/business functions, external mission/business relationships, management/operational policies, procedures, and structures). ■ Exemplary adversarial threat events, annotated by the organisation, if necessary. ■ Exemplary non-adversarial threat events, annotated by the organisation, if necessary. ■ Assessment scale for assessing the relevance of threat events, annotated by the organisation, if necessary. ■ Threat events identified in previous risk assessments, if appropriate.	No	Yes	Yes If not provided by Tier 2
From Tier 2: (Mission/business process level) ■ Threat event information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). ■ Mission/business process-specific characterization of adversarial and non-adversarial threat events.	Yes Via RAR	Yes Via Peer Sharing	Yes
From Tier 3: (Information system level) ■ Threat event information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). ■ Information system-specific characterization of adversarial and non-adversarial threat events. ■ Incident reports.	Yes Via RAR	Yes Via RAR	Yes Via Peer Sharing

Table 9 Examples of adversarial threat events (continues on following pages) (National Institute of Standards and Technology, 2012)

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/ scanning.	Adversary uses commercial or free software to scan organisational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organisational information.	Adversary mines publicly accessible information to gather information about organisational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organisations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organisations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organisational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high-value targets (e.g., senior leaders/ executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organisational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organisations to inject malicious components into the supply chain.	Adversary creates false front organisations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organisational supply chain.
Deliver/insert/install malicious capabilities.	
Deliver known malware to internal organisational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organisational information systems.
Deliver modified malware to internal organisational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organisational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organisational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organisational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organisational information systems.

Threat Events (Characterized by TTPs)	Description
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organisations, simply looking for entry points into internal organisational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organisational information systems and information system components.	Adversary inserts malware into organisational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organisations (based on knowledge gained via reconnaissance).
Insert specialized malware into organisational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organisational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organisational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organisational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organisation-controlled information systems or networks.	Adversary installs sniffing software onto internal organisational information systems or networks.
Install persistent and targeted sniffers on organisational information systems and networks.	Adversary places within internal organisational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organisational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organisations.	Adversary places individuals within organisations who are willing and able to carry out actions to cause harm to organisational missions/business functions.
Insert subverted individuals into privileged positions in organisations.	Adversary places individuals in privileged positions within organisations who are willing and able to carry out actions to cause harm to organisational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise.	
Exploit physical access of authorised staff to gain access to organisational facilities.	Adversary follows ("tailgates") authorised individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Exploit poorly configured or unauthorised information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorised for Internet connectivity or that do not meet organisational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organisational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organisational information systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organisationally used cloud environment, takes advantage of multi-tenancy to observe behavior of organisational processes, acquire organisational information, or interfere with the timely or correct functioning of organisational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organisations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organisational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

Threat Events (Characterized by TTPs)	Description
Exploit vulnerabilities on internal organisational information systems.	Adversary searches for known vulnerabilities in organisational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unplublicised vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organisations as well as adversary reconnaissance of organisations.
Exploit vulnerabilities in information systems timed with organisational mission/business operations tempo.	Adversary launches attacks on organisations in a time and manner consistent with organisational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversary obtains unauthorised information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organisational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organisations for purposes of subsequently infecting organisations when reconnected.
Compromise software of organisational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organisational information systems.
Compromise organisational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organisational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organisations to which information is supplied, from carrying out operations.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorised ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorised for use by organisations.
Conduct attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted Denial of Service (DoS) attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organisational facilities.	Adversary conducts a physical attack on organisational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organisational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organisational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organisational facilities.	Adversary conducts a cyber-physical attack on organisational facilities (e.g., remotely changes HVAC settings).

Threat Events (Characterized by TTPs)	Description
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organisational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organisational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicised vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organisations.
Conduct externally-based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organisations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organisations in order to gain access to organisational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organisations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally-based network traffic modification (man in the middle) attacks.	Adversary, operating outside organisational systems, intercepts/eavesdrops on sessions between organisational and external systems. Adversary then relays messages between organisational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organisational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organisational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organisations into revealing critical/ sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organisations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organisational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organisations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organisations (or organisational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organisational systems to locate and surreptitiously transmit sensitive information.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organisational systems to impair the correct and timely support of organisational mission/business functions.
Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organisational ability to carry out missions or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes, or otherwise makes unauthorised changes to, organisational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organisational data/services.

Threat Events (Characterized by TTPs)	Description
Cause integrity loss by injecting false but believable data into organisational information systems.	Adversary injects false but believable data into organisational information systems, resulting in suboptimal actions or loss of confidence in organisational data/services.
Cause disclosure of critical and/or sensitive information by authorised users.	Adversary induces (e.g., via social engineering) authorised users to inadvertently expose, disclose, or mishandle critical/sensitive information.
Cause unauthorised disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organisational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorised. The information is exposed to individuals who are not authorised access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organisational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organisational wireless routers.
Obtain unauthorised access.	Adversary with authorised access to organisational information systems, gains access to resources that exceeds authorisation.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organisations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organisations or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organisations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organisational security measures.
Coordinate a campaign.	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organisational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organisations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organisation. Adversary observes multiple organisations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organisational systems from existing presence.	Adversary uses existing presence within organisational systems to extend the adversary's span of control to other organisational systems including organisational infrastructure. Adversary thus is in position to further undermine organisational ability to carry out missions/ business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organisational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organisational operations.

Table 10 Examples of non-adversarial threat events (National Institute of Standards and Technology, 2012)

Threat Event	Description
Spill sensitive information	Authorised user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorised to handle. The information is exposed to access by unauthorised individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorised users	Authorised privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorised privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility	Earthquake of organisation-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organisation-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organisation-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organisation-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organisation-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Table 11 Identification of relevance of threat events to the organisation (National Institute of Standards and Technology, 2012)

Value	Description
Confirmed	The threat event or TTP has been seen by the organisation.
Expected	The threat event or TTP has been seen by the organisation's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organisation, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organisation is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

Appendix 3A - Vulnerabilities and predisposing conditions identification

Table 12 Possible inputs to the vulnerabilities and predisposing conditions identification (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organisation level) 🟩 Sources of vulnerability information deemed to be credible (e.g., open source and/or classified vulnerabilities, previous risk/vulnerability assessments, Mission and/or Business Impact Analyses). 🟩 Vulnerability information and guidance specific to Tier 1 (e.g., vulnerabilities related to organisational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/business relationships). 🟩 Taxonomy of predisposing conditions, annotated by the organisation, if necessary. 🟩 Characterization of vulnerabilities and predisposing conditions. 🟩 Assessment scale for assessing the severity of vulnerabilities, annotated by the organisation, if necessary. 🟩 Assessment scale for assessing the pervasiveness of predisposing conditions, annotated by the organisation, if necessary. 🟩 Business Continuity Plan, Continuity of Operations Plan for the organisation, if such plans are defined for the entire organisation.	No	Yes	Yes If not provided by Tier 2
From Tier 2: (Mission/business process level) 🟩 Vulnerability information and guidance specific to Tier 2 (e.g., vulnerabilities related to organisational mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). 🟩 Business Continuity Plans, Continuity of Operations Plans for mission/business processes, if such plans are defined for individual processes or business units.	Yes Via RAR	Yes Via Peer Sharing	Yes
From Tier 3: (Information system level) 🟩 Vulnerability information and guidance specific to Tier 3 (e.g., vulnerabilities related to information systems, information technologies, information system components, applications, networks, environments of operation). 🟩 Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). 🟩 Results of monitoring activities (e.g., automated and nonautomated data feeds). 🟩 Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. 🟩 Contingency Plans, Disaster Recovery Plans, Incident Reports. 🟩 Vendor/manufacturer vulnerability reports.	Yes Via RAR	Yes Via RAR	Yes Via Peer Sharing

Table 13 Threat sources identification and assessment - characteristics of adversary targeting (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to all organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to most organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to many organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to some organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to few organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).

Table 14 Taxonomy of predisposing conditions relevant to vulnerability (National Institute of Standards and Technology, 2012)

Type of Predisposing Condition	Description
INFORMATION-RELATED 🟩 Classified National Security Information 🟩 Compartments 🟩 Controlled Unclassified Information 🟩 Personally Identifiable Information 🟩 Special Access Programs 🟩 Agreement-Determined - NOFORN - Proprietary	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organisational agreements.
TECHNICAL 🟩 Architectural - Compliance with technical standards - Use of specific products or product lines - Solutions for and/or approaches to user-based collaboration and information sharing - Allocation of specific security functionality to common controls 🟩 Functional - Networked multiuser - Single-user - Stand-alone / nonnetworked - Restricted functionality (e.g., communications, sensors, embedded controllers)	Needs to use technologies in specific ways.
OPERATIONAL / ENVIRONMENTAL 🟩 Mobility - Fixed-site (specify location) - Semi-mobile - Land-based, Airborne, Sea-based, Space-based - Mobile (e.g., handheld device) 🟩 Population with physical and/or logical access to components of the information system, mission/business process, EA segment - Size of population - Clearance/vetting of population	Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.

Table 15 Threat sources identification and assessment - characteristics of adversary targeting (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to all organisational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to most organisational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to many organisational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to some organisational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to few organisational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

Appendix 3B - industry standards to support a gap assessment

To determine the current state of the system, the following standards offer more details:

- ISO27001 – Create an asset inventory [source].
- IEC62443-3-2:2020 – offers segmentation methodology for structuring into zones and connections. [source missing]
- NIST-SP800-30 - proposes a system characterisation under the Risk Management guide for information technology systems [source].

To determine the gap and remedial actions, the following standards provide more details.

- IEC 62443-3-3:2019 - introduces the security levels to use in the gap analysis, to address the gaps and suggests a standardised nomenclature. [source missing]
- NIST-SP800-30 - proposes practices to identify vulnerabilities that can also be used for gap classification (source).

Appendix 4 - Risk quantification

Table 16 Example of a risk likelihood scale

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	>10^-1per year (High demand)
2	Likely	Likely to occur	10^-1 to 10^-3per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^-3 to 10^-4 per year
4	Unlikely	Conceivably possible, but very unlikely to occur	10^-4 to 10^-5per year
5	Remote	So unlikely that it can be assumed it will not occur	>10^-5 per year

Table 17 Example of a risk severity scale

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offence	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over a large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanour criminal offence	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by a local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on the community	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Table 18 Example of a risk likelihood – severity matrix

Below are provided some sample risk assessment matrices, which can vary depending on the depth of the analysis. Additional information can be found in [source, IEC 62443-3-2:2020].

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

Table 19 Example of a 3x3 risk matrix

Likelihood	Highly likely	Medium	High	High
	Possible	Low	Medium	High
	Unlikely	Low	Low	Medium
		Negligible	Moderate Impact	Severe

Table 20 Example of a 5x5 risk matrix

		Consequence				
		Minor problem (Easily handled by normal day-to-day processes)	Some distribution possible (Damage between $500k and $1MM)	Significant time and resources required (Damage between $1MM and $10MM)	Operations severly damaged (Damage between $10MM and $25MM)	Business survival at risk (Damage >$25MM)
Likelihood	Almost certain (>90%)	High	High	Extreme	Extreme	Extreme
	Likely (50% - 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (10% - 50%)	Low	Moderate	High	Extreme	Extreme
	Unikely (3% - 10%)	Low	Low	Moderate	Extreme	Extreme
	Rare (>3%)	Low	Low	Moderate	High	High

Table 21 Example of a 5x5 risk matrix

		Severity			
		Minor problem (Easily handled by normal day-to-day processes)	Some distribution possible (Damage between $500k and $1MM)	Significant time and resources required (Damage between $1MM and $10MM)	Operations severly damaged (Damage between $10MM and $25MM)
Likelihood	Imbrobable (Risk is unlikely to occur)	Low - 1 -	Medium - 4 -	Medium - 6 -	High - 10 -
	Likely (50% - 90%)	Low - 1 -	Medium - 5 -	High - 8 -	Extreme - 11 -
	Moderate (10% - 50%)	Medium - 3 -	High - 7 -	High - 9 -	Extreme - 12 -

Table 22 Example of a risk register

Risk ID	Asset	Thread Source/Event	Vulnerability	Impact	Existing Controls	Initial Risk Rating			Responsible person/ Risk Owner	Mitigating Actions	Residual Risk Rating			Notes	Tolerated Risk
						Probability	Severity	Risk Rating			Probability	Severity	Risk Rating		
1															
2															
3															

Appendix 5A- System partitioning & segmentation

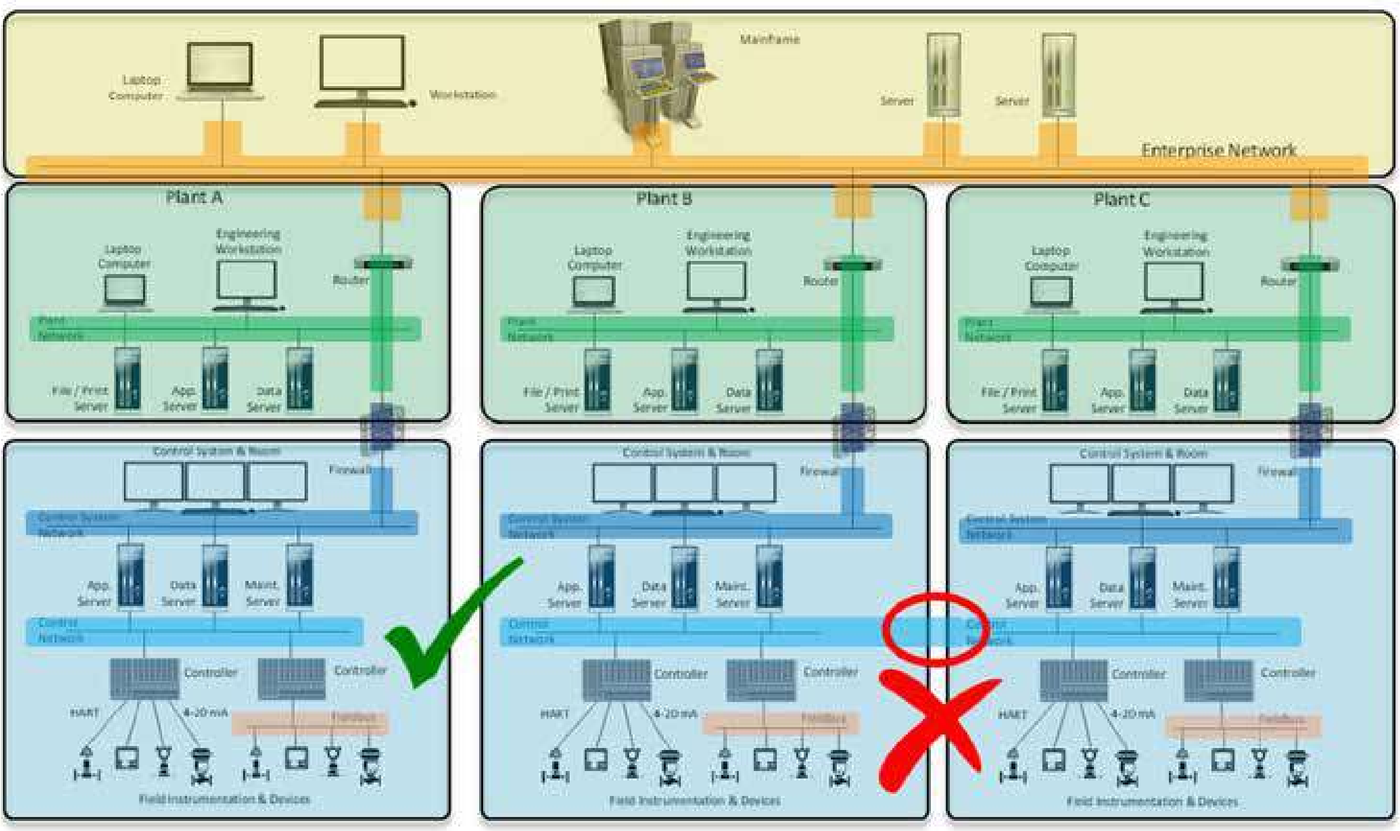


Figure 4 Example of correct and wrong partitioning and segmentation of assets (Source: ISA Global Cybersecurity Alliance)

Appendix 5B - Mitigation strategies & defence-in-depth

Table 23 Recommended solution and strategies for Defence-in-Depth security[xxv]

Defence-in-Depth	Strategy Elements
Risk management	Identify threats Characterise risk and its likelihood Maintain an asset inventory and network architecture
Cyber Security Architecture	Standards/Recommendations Policies Procedures
Physical Security	Mobile electronics locked down Control centre & asset access controls Remote site video security, physical barriers and access controls
Network Architecture & Security	Network Segmentation (Zones & Conduits) Firewalls Remote Access & Authentication
Host Security	Patch Management Virtual Machines Malware & Antivirus Protection Password & Access Controls
Security Monitoring	Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS) Security Audit Logging Security Incident & Event Monitoring (SIEM)
The Human Element	Policies Procedures Training and Awareness

Appendix 5C - Incident response and recovery plan

Backed by clear policies and procedures, a response and recovery plan should prevent the loss of data, decrease the system down-time and allow the company to analyse and recover from the incident, while meeting regulatory requirements if the system affects health, safety or personal information. It should detail which incidents would be covered (generally any adverse cyber event that has a negative impact), the team responsible for taking decisions and responding to the incident, and the company's expectations of them.

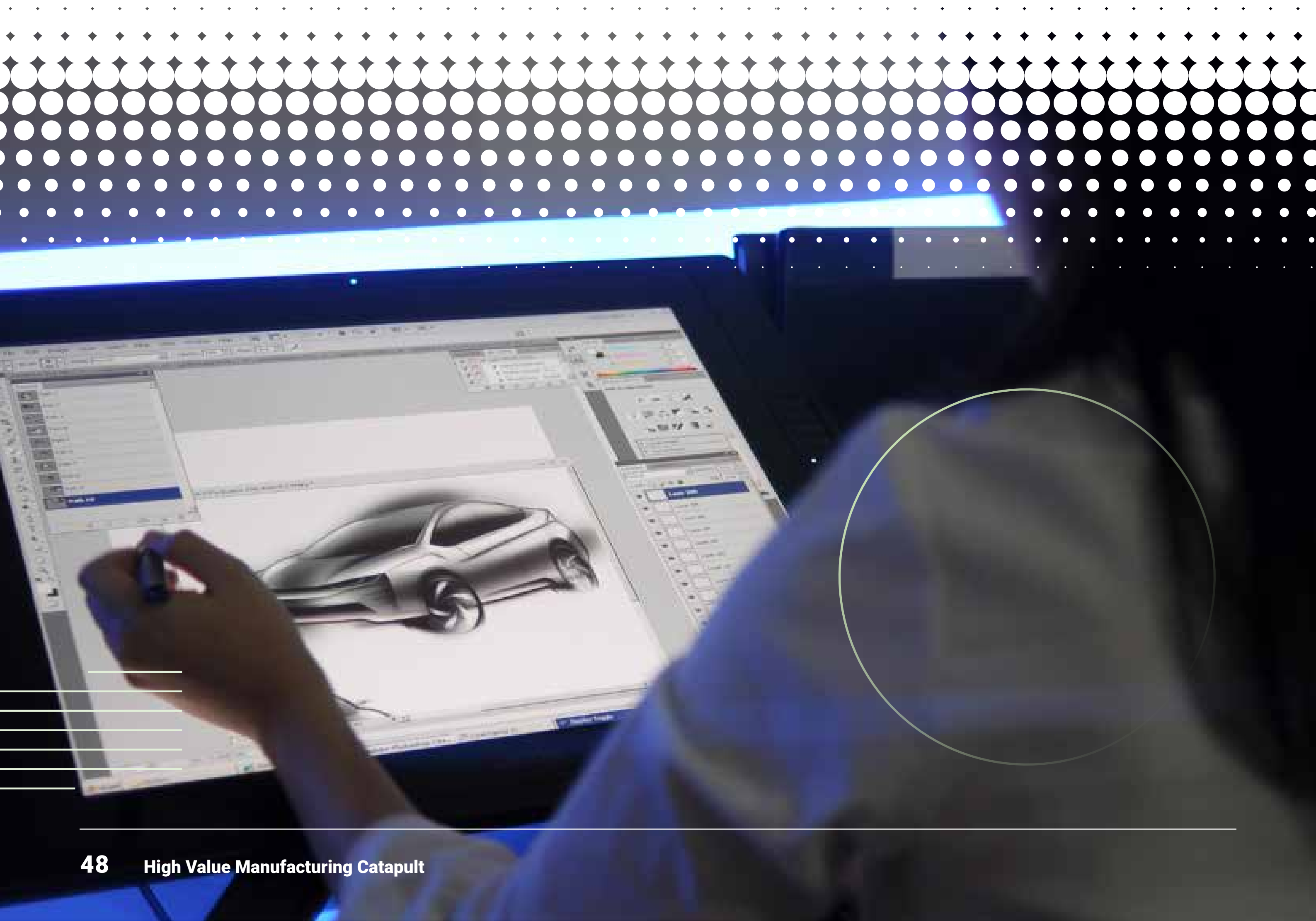
The policies and procedures should include:

- The purpose & objectives of the policy.
- The scope of the policy ("to whom and what it applies and under what circumstances").
- The definition of a security incident or breach and any related terms.
- The incident team's organisational structure, responsibilities and authority.
- The levels of communication (e.g. how/when the incident team should interact with third parties such as law enforcement, media, incident response teams, etc.)
- The severity and priority rating for incidents.
- Performance measures.
- Reporting procedures and contact details.

The response plan should contain specific practical elements, such as:

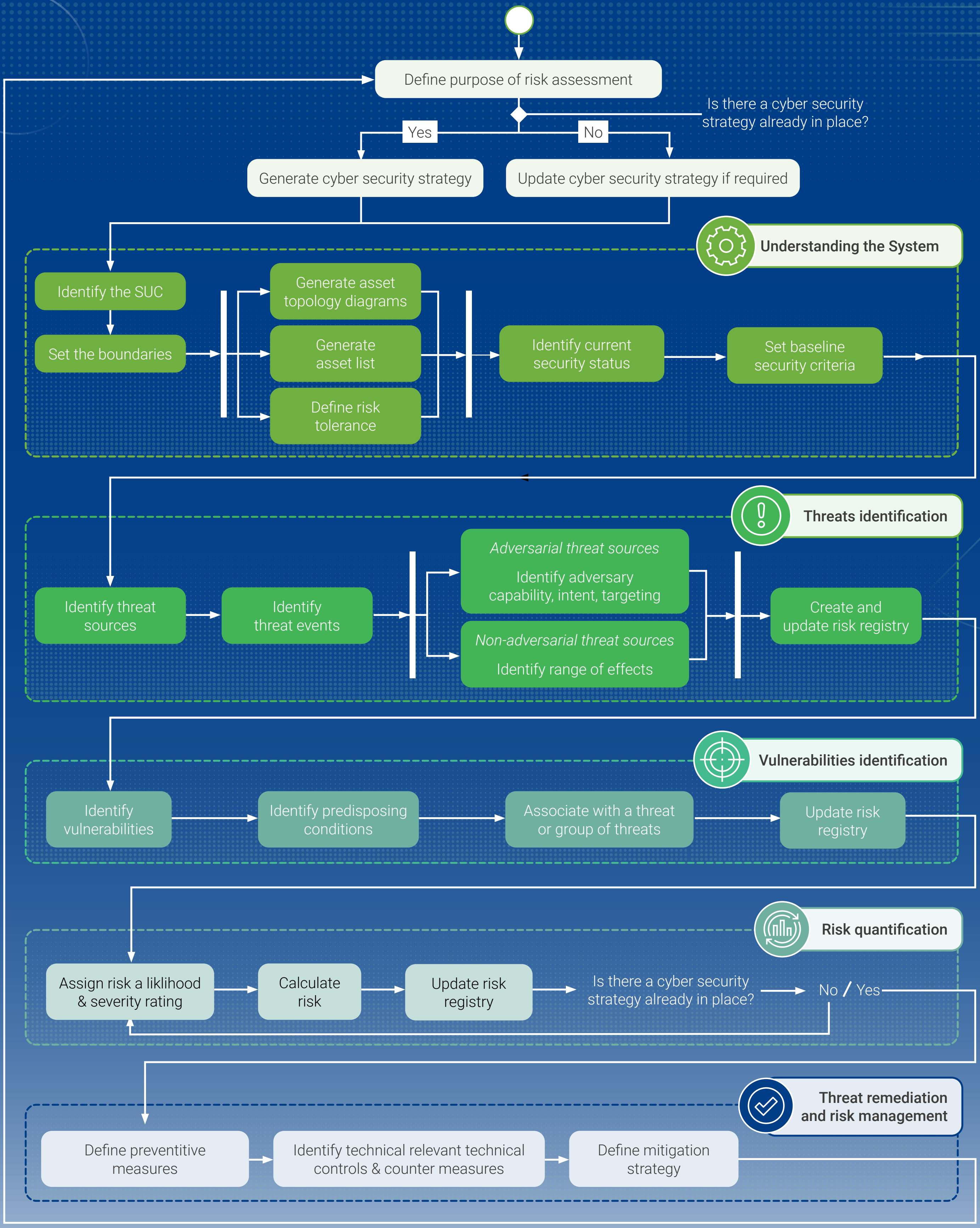
- Key contacts and their hierarchy.
- The initial risk assessment to identify vulnerabilities and any analysis of past incidents.
- How to ensure secure back-ups are maintained.
- How to contain or eradicate damage from different types of incidents.
- How to start identifying and recovering elements that have become corrupted or vulnerable.
- How to restore the system to its normal state (eg using the backup, rebuilding, patches, replacing files) and potential timeframes (can be anything from a few days to a few months).
- An overview of the above processes.
- Steps and timeframes to carry out a post-incident review including collating data, learning lessons and recommending actions to improve security.

Containing a breach doesn't prevent it from causing damage elsewhere, so the review should include both the original vulnerability that caused the incident and any new vulnerabilities that may have created.



Appendix 6 - Overview

Figure 5 Flowchart of the actions contained in this assessment framework


Define purpose of risk assessment
Is there a cyber security strategy already in place?
Yes
No
Generate cyber security strategy
Update cyber security strategy if required
Understanding the System
Identify the SUC
Set the boundaries
Generate asset topology diagrams
Generate asset list
Define risk tolerance
Identify current security status
Set baseline security criteria
Threats identification
Identify threat sources
Identify threat events
Adversarial threat sources
Identify adversary capability, intent, targeting
Non-adversarial threat sources
Identify range of effects
Create and update risk registry
Vulnerabilities identification
Identify vulnerabilities
Identify predisposing conditions
Associate with a threat or group of threats
Update risk registry
Risk quantification
Assign risk a liklihood & severity rating
Calculate risk
Update risk registry
Is there a cyber security strategy already in place?
No / Yes
Threat remediation and risk management
Define preventitive measures
Identify technical relevant technical controls & counter measures
Define mitigation strategy

References

[i] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[ii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[iii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[iv] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[v] Risk assessments can be carried out at three different levels of a business, according to the standard NIST 800-30 (section 2.4, p17);

[vi] Risk assessments can be carried out at three different levels of a business, according to the standard NIST 800-30 (section 2.4, p17);

[vii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[viii] NIST 800-30

[ix] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/why-your-cyber-risk-tolerance-may-be-lower-than-you-think/

[x] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[xi] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[xii] https://dig8ital.com/resources/library/its-time-to-identify-your-cyber-security-risk-appetite#:~:text=What%20is%20cyber%20risk%20appetite,the%20confidentiality%20of%20customer%20data

[xiii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[xiv] https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

[xv] https://www.langner.com/2019/02/the-five-things-you-need-to-know-about-ot-ics-vulnerability-and-patch-management

[xvi] https://gca.isa.org/blog/how-to-define-zones-and-conduits

[xvii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[xviii] https://www.ciscopress.com/articles/article.asp?p=1336425

[xix] https://www.dnsstuff.com/network-intrusion-detection-software

[xx] https://www.gartner.com/reviews/market/security-information-event-management

[xxi] https://www.splunk.com/pdfs/ebooks/the-siem-buyers-guide-for-2020.pdf

[xxii] https://www.splunk.com/pdfs/ebooks/the-siem-buyers-guide-for-2020.pdf

[xxiii] https://www.ncsc.gov.uk/pdfs/information/reducing-your-exposure-to-cyber-attack.pdf

[xxiv] https://csrc.nist.gov/glossary/term/Acceptable_Risk

[xxv] https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf