Chapter 4
Cyber-Resilience, Principles, and Practices

Hilary Meagher and Lubna Luxmi Dhirani

4.1 Introduction

In a world where sophisticated technologies have fully reformed ways of communication, healthcare, manufacturing, etc., has increased the need for securing these digitally transformed environments as well [1]. As per recent statistics, 5.3 billion people across the world use the Internet; public cloud usage has increased, and cloud spending has touched the $490.3 billion mark [2]. The Industrial Control Systems Operational Technology (ICS-OT) cyber-attacks surged by 60%, and 1,300 ICS-specific vulnerabilities were identified [3], the majority of which had high to critical severity ratings. It is anticipated that by 2030, more than 29 billion IoT devices will be used for industrial and commercial use; cloud dependencies on Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) and usage will grow beyond 200 zettabyte [4]. Internet of Everything (IoE) is one of the examples that emerged with new integrated technologies and communication systems. This is merely an example of the data-driven digital economy and markets we are heading toward. In the past few years, manufacturing industries have been the most exploited and cyber-extorted environments by malicious actors with the intention of gaining financial advantages, espionage, intellectual property theft, etc. These threats would potentially escalate with the use of

H. Meagher
Department of Electronic & Computer Engineering, University of Limerick (UL), Limerick, Ireland

L. L. Dhirani (✉)
Department of Electronic & Computer Engineering, University of Limerick (UL), Limerick, Ireland

Confirm—SFI Smart Manufacturing Centre, Limerick, Ireland
e-mail: lubna.luxmi@ul.ie

K. Naseer Qureshi et al. (eds.), *Cybersecurity Vigilance and Security Engineering of Internet of Everything*, Internet of Things,
https://doi.org/10.1007/978-3-031-45162-1_4

emerging technologies like IoE, as standards to control and mitigate these threats have not been fully developed. As the cyber-threat landscape is constantly changing and new threats are coming to the surface, in such a scenario, a systematic cybersecurity framework is required to identify, assess, align, mitigate, and build cyber-resilience in the environment.

To protect the manufacturing environment from increasing vulnerabilities and threats, there is a pressing need for strong cyber-policies, laws, and controls especially for IoE smart industry networks. The European Union has developed new regulations and frameworks (i.e., EU Cybersecurity Act 2022, EU Cybersecurity Strategy, EU Cyber Resilience Act 2022, EU Digital Markets Act, EU Digital Fairness Act, Network and Information Security 2-Directive (NIS2-D), General Data Protection Regulation (GDPR), Cyber Diplomacy Toolbox 2022, and 5G Toolbox [5–7]) for mitigating cyber and geopolitical risks. The war between Russia and Ukraine has demonstrated that cyber-wars could cause more damage than the ones fought at the line of control at the border. The goal of a cyber-war is to use digital technologies for hacking and targeting military, government networks, and critical infrastructure, such as power grids or transportation systems, disrupting communications, jeopardizing the availability of services (i.e., triggering economic and operational disruption), and affecting human lives [8]. These cyber-attacks are usually carried out by infiltrating the command and control (C&C), installing malware, or launching distributed denial-of-service (DDoS) type of attacks [8].

A report in [9] states that more than 45% of industries have insufficient security measures. This shows the majority of industries have no effective incident response or mitigation process in place. There could be a number of reasons to blame such negligence (i.e., lack of skilled staff, policies, security controls, measures, standards, compliance, etc.). Considering the cost related to escalating cybercrime and attacks (i.e., man-in-the-middle, crypto-jacking, phishing, third-party, software and hardware vulnerabilities, ransomware, etc.) happening at different levels in the manufacturing supply chain, if these risks are not neutralized and mitigated, they could cause massive safety, security, operational downtime, and financial consequences. Stolen intellectual property (IP) can cost manufacturing industries more than 3,000 million dollars, reputational damage, legal and litigation costs, and lost customers.

As per the new European Regulations, building cyber-resilient within infrastructures is now mandatory for industries operating in the European jurisdiction. Some of the challenges to reaching the cyber-resilient goals are as follows: (i) cross-domain interoperable standards for emerging technologies; (ii) gap analysis; (iii) regulatory and legal compliance; (iv) enforcing policies, auditing, and having an incident response plan; and (v) easing trade across Europe [9]. To secure an environment, it is essential to fully understand the technological infrastructure, operations, dependencies, resources, and flow of data.

This chapter provides a roadmap for building cyber-resilience within an industry by the following:

(i) Identifying, assessing, and aligning cybersecurity standards across the manufacturing plant
(ii) Enabling cross-platform standard alignment

Fig. 4.1 Building cyber-resilience using CYBER INTEL framework

(iii) Designing and mapping the cybersecurity strategy with the statutory, regulatory, and contractual standards
(iv) Gap analysis and threat mitigation
(v) Enforcing strong technical, operational, and political policies
(vi) Auditing and having an incident response in place
(vii) Enabling a trust-based manufacturing environment, easing international trade

The chapter is categorized in the following sections as shown in Fig. 4.1.

Section 4.2 introduces the authors' designed cybersecurity framework for building cyber-resilience. The section is further divided into ten parts that demonstrate mapping with the statutory, legal, regulatory, and contractual standards and controls. It also provides implementation using a use-case example. Section 4.3 provides a reflective summary of the chapter and future directions.

4.2 Building Cyber-Resilience in Industry Using CYBER INTEL

As technology continues to advance, the threat of cyber-war is becoming increasingly real. Critical infrastructures, industries, militaries, and governments around the world are investing heavily in cybersecurity, developing tools and strategies to defend against cyber-attacks. This chapter introduces an authors' designed "CYBER INTEL (CYBERsecurIty staNdards, risk assessment, Threat Intelligence, Legal, and rEgulatory) framework that aligns cyber-laws and regulations, together with compliance standards and frameworks, auditing, and controls required to protect

industries from the impacts of cyber-attacks. The framework provides a roadmap for selecting and employing appropriate cybersecurity standards and baseline security metrics and defines strategies for risk management and compliance with cybersecurity frameworks. The framework presents guidance for aligning related cybersecurity regulations and laws in protecting critical assets. It also provides oversight on how to build cyber-resilience in an industry. It touches on incident response planning and highlights the need for security awareness training, risk assessments, and auditing to ensure that companies are compliant with defined controls, standards, laws, and regulations that have been implemented to protect the company from cyber-crime.

4.2.1 Traction Plc. (Selected Use-Case)

For demonstrating a working example, the authors chose to use a fictional Manufacturing plant model to base the use-case on. The use-case (Traction Plc.) is derived from the author's exposure and experience gained working in the Supply Chain Manufacturing sector over the past 15+ years and disseminates valuable insights. There were data protection regulations and security issues with sharing information related to real manufacturing environment, so the authors felt that a use-case would be an appropriate choice.

Traction Plc. is a manufacturing company based in Ireland. It has three manufacturing plants located in Galway, Dublin, and Cork all of which are connected via a company Wide Area Network (WAN) which is managed by a third-party service provider [10]. Each site has a Local Area Network (LAN) and share a common enterprise domain. The enterprise ERP solution is hosted at the head quarter plant in Dublin, critical data used in this solution is encrypted at rest. Connections are managed via web services, and these are encrypted in motion using Secure Socket Layer (SSL) certs.

The Industrial Control System (ICS) network and supporting services have been segregated in line with the ISA-95 Purdue model. Each plant has its own separate physical and logical network with a common Manufacturing domain across all three. Site network perimeter firewalls are configured with content inspection enabled. Network switches are configured with Network Access Control (NAC), port security and Dynamic Host Configuration Protocol (DHCP) guard to prevent unauthorized access and unauthorized DHCP servers on the network [11]. Switch configurations are backed up using SolarWinds Network Configuration Manager to ensure recoverability. Communications into and out of the ICS network are protected by a demilitarized zone (DMZ) with firewalls. Each plant has between 5 and 10 process areas, each with its own Programmable Logic Controller (PLC) controller and a fieldbus network with various sensors and actuators. PLC firmware is updated on a regular basis in line with vendor recommendations. There is a supervisory level SCADA solution local to each plant which is used to control the processes. This interacts directly with Level 0 devices via local HMI's. ICS traffic is

isolated using dedicated virtual local area networks (vLAN) per process area which are configured to limit inter-vLAN communications.

Remote access for maintenance and support is managed via a secured solution which allows connectivity through a virtual private network (VPN) connection and limits access to defined IP's and ports based on predefined requirements and multi-factor authentication. A remote desktop services (RDS) server is hosted in the DMZ and vendors with appropriate authorized access can jump to an Engineering workstation at Level 3 which has several OT applications installed to allow Engineering teams configure and maintain Level 0 and Level 1 devices. All sites have a local industrial backup and recovery solution for backing up PLC code and firmware, vendor human machine interface's (HMI) and managed Industrial switches. Servers are backed up nightly by a site backup and recovery solution with encrypted backups. Anti-virus, end point protection and regular operating system (OS) patching is in place on all Wintel devices with emergency patching for high-risk vulnerabilities catered for with an out-of-band patching cycle. Enterprise and ICS applications are kept patched up to date in line with vendor recommendations.

4.2.2 Cyber-Threat Landscape

According to a 2019 study conducted by Forrestor Consulting on behalf of Armis, "*66% of manufacturing firms have encountered an IoT-related security incident*" [12]. Major impacts from a cyber-attack on manufacturing companies include data breach, loss of intellectual property, disruption and downtime leading to financial loss and reputational damage. Majority of the ICS systems are not based on the security by design principles. This flaw would allow broader gaps within the environment, exploiting it to a broader threat landscape. Traction Plc is potentially vulnerable to threats related to legacy equipment, operating systems and software vulnerabilities, lack of network micro-segmentation and configuration issues. The attack surface stretches down to the lower levels of an ICS network where an attacker with physical access could potentially use direct access cards or chips that are plugged into a device to scan for and exploit un-remediated vulnerabilities. Maintenance interfaces with no authentication can be used to gain access and control of PLC's, opening the door for an attacker to program bad inputs into a controller to change how a process is running, or indeed the components or quantities of a recipe used by a process to manufacture a product.

4.2.3 Data Security and Risk Management

Historically, ICS systems have lacked security in their design and leading to a wider attack surface which leaves them vulnerable to attacks such as an ICS or IT Insider, common, targeted or zero-day ransomware, Industrial IoT (IIoT) pivot, vendor back

door [13]. To protect against the risks mentioned in Sect. 2.2, a robust data risk management strategy is required. *"Building a mitigation and prevention strategy that centers on security, vigilance and resilience can be key toward managing risk"*[14]. A starting point to building out that strategy is understanding the technology and solutions landscape that needs to be protected. This, together with the data stored and processed in the environment, are critical to business processes and therefore need security and appropriate controls in place to protect them. Consideration should be given to the three common blocks of security which comprise the security (confidentiality, integrity and availability (CIA triad)) when designing any data risk management strategy. Use of an industry standard framework such as the NIST Risk Management Framework (RMF) is a good foundation and can be tailored to suit business needs [15].

For Traction Plc., the manufacturing company described in the use-case outlined above, a data risk management plan includes the following:

(i) Defining the key data risk management roles and responsibilities to ensure the right level of accountability and ownership is in place.
(ii) Generating a detailed asset inventory of both IT and OT systems and devices such as servers, workstations, HMI's, PLC's, scan guns, printers, network switches, in-house developed applications, Commercial off-the-shelf (COTS) software applications, licenses, etc. It includes asset details such as name, hardware type, IP address, operating system, firmware etc. User access information is made available, through Active Directory where applications are configured with lightweight directory access protocol (LDAP) or similar, or through a manual list that details the local users configured on a device and their level of access. *"High value assets and high impact systems that require increased levels of protection"*[16] are identified as part of this process.
(iii) Identifying the data hosted and processed by all systems used to support Manufacturing processes including those where there is integration between the IT and OT systems. Data is classified according to a defined data classification policy (Public, Internal, Confidential, Sensitive).
(iv) Performing a cyber-risk assessment for evaluating current security posture, including both organization and systems in line with recommendations from NIST RMF. Findings are used for identifying current known cyber-risks and an actionable plan to address is built out, taking people, process, and technology impacts into account. The cyber-risk assessment is a bi-annual exercise and requires alignment with business leaders across key functions e.g. Engineering, automation, maintenance, supply chain operations, information technology, information security, etc.
(v) Choosing appropriate security and privacy controls to protect the systems based on the results of the risk assessment. Suitable controls are applied across the various business process areas to address identified risks, in alignment with the NIST Cyber Security framework and mapped to the center for internet security (CIS) Controls ensuring appropriate coverage to meet identi-

fied business risks e.g., backup and recovery, asset management, compliance management, system security, physical security, operations, disaster recovery.

(vi) Identifying resources with ownership and accountability for the controls.

(vii) Implementing the controls and ensuring process documents are complete. A detailed description of the risk and objective of the control, and the associated execution steps are required to ensure there is clarity for the assigned control and process owners who are responsible for executing and reporting the control results.

(viii) Assessing the controls after a certain period of time to ensure they are working as expected and producing the desired outcomes.

(ix) Defining and rolling out a regular process to monitor the effectiveness of the controls and ensuring they operate as expected. This should encompass mitigation activities and redesign of control processes where areas of opportunity are identified as part of regular monitoring.

4.2.4 Cyber and Data Protection Laws & Regulations

The high-level plan outlined above provides a foundational approach for protecting Traction Plc's assets. To strengthen this data risk management strategy, several cyber-laws have been defined and enacted under Irish and European Law which "*provide for various cybercrimes like hacking, phishing, electronic theft, etc. Ireland also has a multitude of laws governing data protection and privacy laws"* [30]. The core purpose of these laws is to protect critical data. For Traction Plc. which is hosted in Ireland, the following laws are applicable, and the company will need to comply with their directives:

(i) *Criminal Justice (Offences Relating to Information Systems) Act 2017*: this Act provides legislation to protect against common cyber-attacks such as hacking, malware, denial of service, identity theft/fraud as well as others. This is applicable for Traction Plc. as the likelihood that the company will experience a cyber-attack at some point is high. This Act supports legal recourse for cybercrimes [17].

(ii) *Data Protection Act 2018 (GDPR):* Traction Plc. needs to handle employee and supplier information during its standard business operations. GDPR governs how this type of personal data is controlled, processed, and stored, and governs privacy rights for an individual [18].

(iii) *EU Cyber Security Act (2019):* this Act established an EU framework for certification of digital products and services in Europe. This ensures a common cybersecurity certification approach in Europe and ultimately, improving cybersecurity in a broad range of products and services [19]. This applies to the network services provided by the third-party service provider in the use-case above, and is also applicable to any ICT products purchased by Traction Plc.

(iv) *E-Privacy (S.I No. 336/2011) European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011:* this law regulates the way that public telecommunications network providers or services handle personal and private data. In the above use-case, the third party who are responsible for managing the company WAN would need to be compliant with this law [20].
(v) *NIS2-Directive*: this legislation *"sets the baseline for cybersecurity risk management measures and reporting obligations"* and will *"further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole"* [21]. As a manufacturer based in Ireland, Traction Plc. must comply with the cybersecurity regulations enforced by this law and will need to be able to demonstrate compliance.
(vi) *EU Cyber Security Resilience Act 2022*: while not yet enacted, a proposal has been shared by the European Commission to put regulations in place to ensure that all digital products are secure by design and are kept secure throughout their lifecycle. As a consumer of digital products, Traction Plc. will need to comply with this Act and ensure that digital products are kept secure, in line with Manufacturer recommendations e.g. patched up to date, hardened [22].

4.2.5 Governance, Risk and Control – Data Protection

Based on the results of an assessment completed using the GDPR Temperature Tool [23], Traction Plc. are considered at low risk of potential exposure to GDPR sanctions (see Fig. 4.2 below). The company operates only in Ireland and does not transfer data outside the EU. Several focus areas were identified that need further review and a plan put in place to address. These include:

(i) Train employees on processing of personal data.
(ii) Complete a risk assessment on processing activities that are carried out.
(iii) Complete a Data Protection Impact Assessment (DPIA) for those processing activities which are subject to same, based on GDPR guidelines.
(iv) Confirm if Traction Plc. are required to keep records of processing activities.

4.2.6 NIST Risk Management Framework

The NIST Risk Management Framework (NIST RMF) provides a comprehensive, flexible, repeatable, and measurable 7-step process (preparing, categorizing, selecting, implementing, assessing, authorizing and monitoring the environment) [24]. This framework was considered because it aligned with Traction Plc. business and security needs.

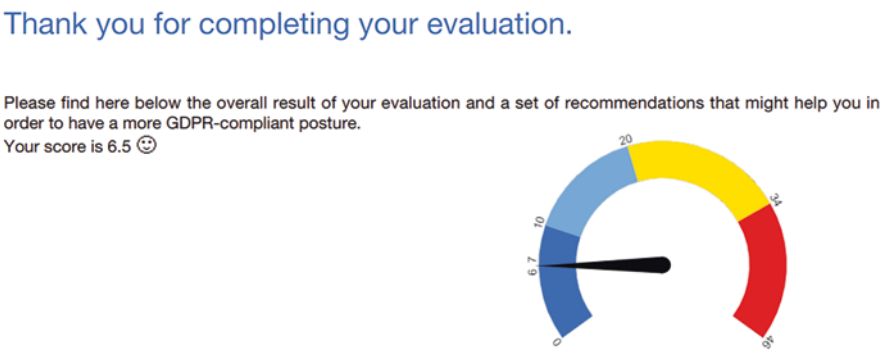

Fig. 4.2 GDPR Temperature Tool results

As the critical assets were identified in Sect. 2.3 (mentioned in i-ix), security measures related to preparing Traction Plc. for managing information security and privacy risks, categorizing critical assets based on impact analysis, selecting and applying relevant controls (NIST 800-53), evaluating the efficacy of the controls, assigned process owners who had authority for risk-based decision and continuously monitoring the controls implemented and risk matrix.

Traction Plc. had taken a proactive approach, identified the need for a risk management framework and implemented the controls before moving to the regulatory and legal frameworks. This helped the manufacturing plant in converging and smoothly aligning with the data security, statutory and regulatory controls (e-Privacy, GDPR, NIS2D, Criminal Justice (Offences Relating to Information Systems) Act 2017, National Cyber Security Strategy 2019-2024, EU Cybersecurity Act.

4.2.7 Incident Response Planning

One of the main components that underpin a strong cyber-resilience strategy is having a well-defined, robust incident response plan to enable companies react to and recover following a cyber-attack such as ransomware, malware, data breach etc. The

plan is typically a *"written set of guidelines that instructs teams on how to prepare for, identify, respond to, and how to recover from a cyber-attack"* [25].

The NIST Computer Security Incident Handling Guide outlines a four-step process for managing incidents. It is worth noting that *"incident response is not a linear activity that starts when an incident is detected and ends with eradication and recovery. Rather, incident response is a cyclical activity, where there is continuing learning and improvement to discover how to better defend the organization"* [26]. This process is used to develop a cyber-incident response plan for Traction Plc. and includes the following steps:

4.2.7.1 Preparation

(v) Identifying key resources to form a Computer Security Incident Response Team (CSIRT) [27], training is provided to ensure resources are informed of their roles and responsibilities in the event of a cyber-incident.
(vi) Generating a repository of recovery documentation and storing an easily accessible and offline/offsite location. This could include an incident response plan, architecture documents, an inventory of critical assets with documented priority, data classification and recovery methods, copy of software licenses, backups for compute, network and OT assets, list of key vendors etc. These documents are reviewed and updated on a regular basis.
(vii) Defining clear steps to be followed if an employee notices suspicious cyber-activity.

4.2.7.2 Detection and Analysis

(i) Collect and review available data from internal and external sources to determine the type of threat per NIST guidelines (precursors and indicators).
(ii) Perform a detailed analysis to identify the vulnerabilities that have been exploited and document and prioritize post-incident actions, ensuring that an audit trail of evidence is maintained.
(iii) Prioritize the approach to handling the incident in terms of functional impact, informational impact, and recoverability.
(iv) Notify impacted parties including reporting to *"appropriate agencies, law enforcement, and any other affected parties"*.

4.2.7.3 Containment, Eradication and Recovery

(i) While the strategy for containing the incident may vary depending on the attack vector, the main objective is to stop the attack and prevent it from further damaging Traction Plc's assets and/or data. Gathering evidence and identifying the attacking hosts are key.

(ii) Following successful containment, the CSIRT team's focus moves to *"eradicating the threat, including removing malware and deleting compromised accounts"*.
(iii) Finally, a phased recovery begins *"which includes cybersecurity patches and taking steps to improve firewalls, reinstall anti-malware, restore systems from clean backups, and changing passwords across the organization"*.

4.2.7.4 Post Incident Activity

(i) A formal session is held to review the incident in depth, learn from challenges encountered during resolution, identify areas for improvement, validate all key stakeholders are part of the process and ensure incident response documentation is updated. This enables a Traction Plc to develop their *"security measures and indeed the incident handling process itself"*.

In general, it is good practice to run regular simulated cyber-incident response exercises where typical cyber-attack scenarios are played out with engagement from key stakeholders. The primary goal is to ensure cyber-recovery plans are tested, validated, and proven to demonstrate confidence in the business's defined and documented recovery procedures. Supporting this activity is regular testing of recovery from backups for compute, network, applications, OT assets, etc. A secondary output is enabling the business to develop an understanding of the average time it would take for Traction Plc. to recover from an incident. In addition, an enterprise-level business continuity plan (BCP) exists which outlines the ability to shift manufacturing capabilities from one plant to another in the event of a major crisis that results in an entire plant being destroyed. This plan also addresses supply risks from third-party suppliers and identifies a list of vetted alternates for critical materials.

If Traction Plc. were to detect a ransomware attack targeting HMIs, this would result in a high impact on operations as manufacturing would be stopped, with potentially significant financial and reputational impacts for the company. However, there is a well-defined incident response plan and a trained CSIRT team who will respond to the incident, containing and eradicating the malware. There are validated offsite copies of backups that can be used to restore HMIs, PLCs, and the Industrial switches used to enable connectivity for the process areas. As the ICS network is segmented, and traffic is contained using dedicated vLANs per process area, the risk of lateral movement is diminished. An attack on one location can be isolated to that location by virtue of the fact that the SCADA solutions are local to each plant and there is no cross-plant communication at the ICS layer.

While external shock factors such as domestic state-sponsored crime or armed conflict are unlikely to have an impact on Traction Plc., due to its location in Ireland, a resource impact cannot be ruled out due to the current macroeconomic climate. From a legal perspective, Traction Plc. is compliant with the Criminal Justice (Offences Relating to Information Systems) Act 2017 and could use legal means to gain recourse in the event of a breach.

4.3 Cybersecurity Compliance

Cybersecurity compliance refers to protecting data security, availability, and integrity. Tools such as the NIST CSF [28] enable to assess of Traction Plc's current security posture and develop a plan for managing cyber-risk. For small and medium-sized businesses like Traction Plc, the simplicity, and flexibility of the NIST CSF proves to be valuable. Traction Plc. used the Axio360 tool for implementing the NIST CSF, aligning and mapping it with NIST 800-53 (controls), IEC62443 [1], GDPR, and other required standards.

Based on the results of the Axio360 report (see Fig. 4.3 below), and understanding that developing a strong cybersecurity program is a critical but difficult task, as the global threat landscape continues to grow. Though various risks and weaknesses in the report were identified, the ones with high-risk impact required immediate attention and are mentioned below:

(i) Review the company's approach to supply chain risk management. Currently there was no defined process for assessing the cybersecurity posture of third-party partners and vendors. It was noted that consideration should be given to define a third party vendor management program including regular risk assessments, as the potential for significant impact from a breach of a third party is an unknown without this layer of governance in place.
(ii) Traction Plc. currently has limited capabilities around detection of events/anomalies and understanding their potential impact. While SolarWinds Orion is in place, it is more of a tactical monitoring tool which does not have advanced threat detection, at this stage proof of concept Security information and event management (SIEM) products such as AlienVault, Qualys, and QRadar. would benefit and increase visibility in this area.
(iii) While some work has already been done in crisis management, the report shows gaps in few processes. Engagement of external consultants who specialize in this area may be a good investment for Traction Plc.

4.4 Governance, Risk & Compliance – Audit Assurance

Earlier in the chapter we discussed a set of security and privacy controls that are implemented for protecting Traction Plc., based on the findings from a cyber-risk assessment. These controls cover multiple business processes, encompassing areas such as system security, physical security, configuration management, operations, backup and recovery, disaster recovery etc. Control techniques and test scripts were defined, control and process owners identified, and a regular monitoring process put in place to ensure compliance. These controls were based on NIST CSF standards but are also mapped across the CIS Controls.

The purpose of a cybersecurity audit is to carry out a "systematic and independent examination of an organization's cybersecurity and to ensure that the proper

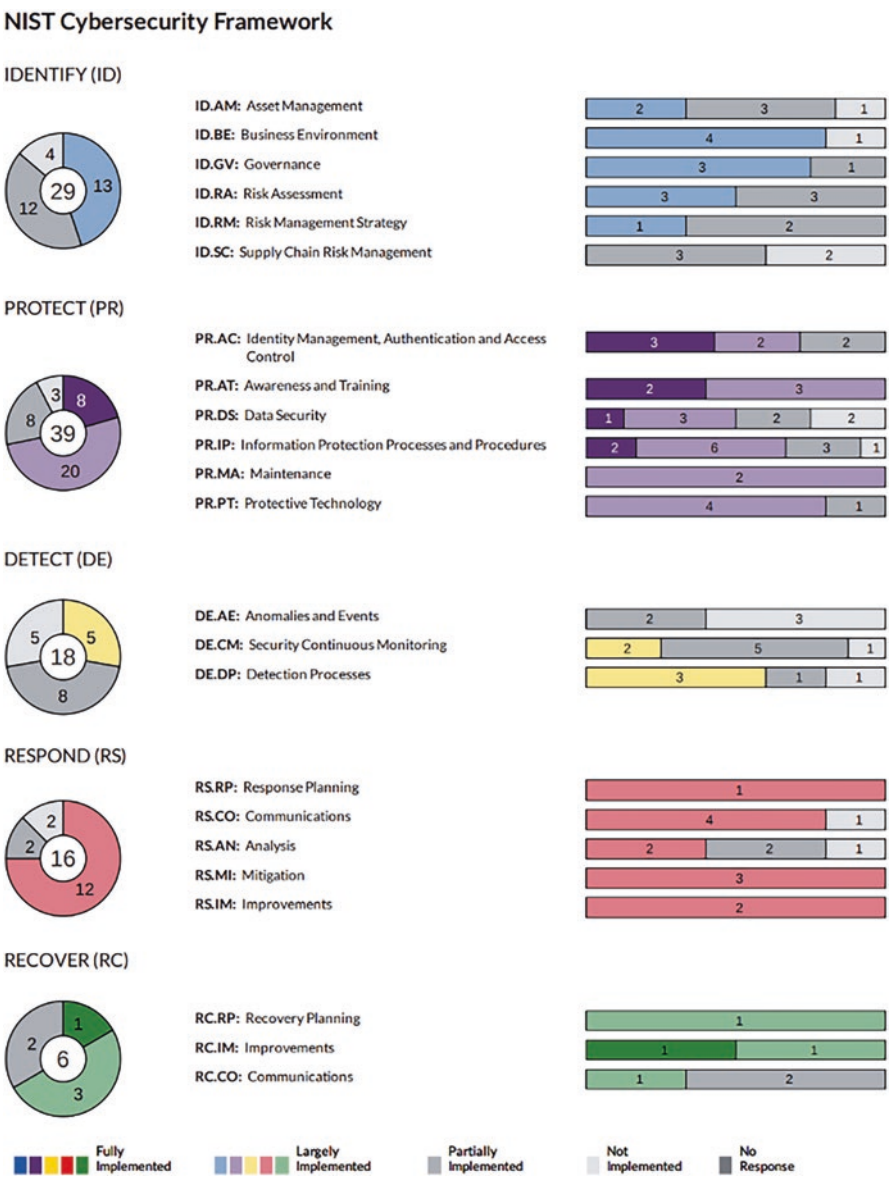

Fig. 4.3 Traction Plc's Cybersecurity posture after implementing the security standards, the gaps mentioned can be seen. These gaps identified can be easily mitigated by using the steps mentioned in Cyber INTEL framework (see 2.8 (i-iii))

security controls, policies and procedures are in place and working effectively". Engaging a third party to perform an independent audit has significant benefits, including providing assurance to the business that governance, risk, and control

processes are in place and are compliant with standards and regulations. There is the added benefit of discovering potential risks or compliance issues that may exist. Audits are typically mandatory for companies to prove compliance with industry cybersecurity frameworks and laws e.g., NIST CSF, CIS, GDPR etc. There are several standards available that can be audited against, SSAE-18 and AT-101 are two such standards which can be used *"to review controls of technology Vendors and other Service Providers"* [28].

4.5 Cyber-Resilience

Cyber-Resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber-resources. It brings "business continuity, information systems security and organization resilience together" [29]. All areas discussed so far form part of an overall cyber-resilience strategy for Traction Plc. However, there is always room for improvement when it comes to cybersecurity and we can build on the NIST RMF [27] data risk management strategy discussed earlier in this chapter, using the five NIST Cyber Security Framework (CSF) functions – Identify, Protect, Detect, Respond and Recover. Note that Traction Plc. is not a FinTech, US government agency or healthcare provider and so compliance standards such as DORA, FedRAMP, e-PHI, and HIPAA. are not applicable for this use-case. Some actions that would provide the most benefit for Traction Plc. include the following:

(i) Develop information security policies to ensure roles and responsibilities are well defined for anyone with access to critical data, including safe disposal of assets (hardware, software, data) which are end of life.
(ii) Develop a regular security awareness training program for all employees, to ensure resources have a good level of awareness around suspicious activity.
(iii) Implement an advanced threat detection monitoring solution to allow Traction Plc. build up a *"baseline of expected data flows and operations for systems and users"* and enable analysis of "*detected threat events to better understand attack methods and targets"*. Both a Host-based Intrusion Detection/Prevention System (HIDS/HIPS) such as Splunk, Symantec Data Centre Security or Palo Alto Cortex XDR, and a Network-based Intrusion Detection System (NIDS) such as Snort or Splunk, should be considered.
(iv) Develop a strong incident response plan to empower business continuity in the event of a cyber-attack.
(v) Consider engaging a reputable third party to conduct annual penetration testing to validate current security posture and identify any potential vulnerabilities.

4.6 Enhanced Cybersecurity Posture Achieved Using the CYBER INTEL Framework

In this chapter, the authors selected a use-case manufacturing company and assessed its security posture using an overview of the foundational security layers, tools, and processes that were in place to protect Traction Plc's critical business assets. The authors developed an awareness of the types of cyber threats that this use-case would be susceptible to and applied a Defense-In-Depth security strategy using the CYBER INTEL framework (based on cybersecurity standards, regulatory compliance frameworks, and cyber-laws and regulations) to secure the ICS environment. Below is a brief synopsis of the areas that have been strengthened:

(i) A data risk management strategy was developed which focused on protecting critical assets and data and mitigating against cybersecurity risks. This strategy involved defining a RACI (responsible, accountable, consulter, and informed) matrix, compiling an asset inventory, identifying and classifying data, performing a cyber-risk assessment to identify current cyber-risks, building out an actionable plan, and implementing appropriate security and privacy controls, including regular monitoring.
(ii) Compliance with industry-relevant cyber-laws, e.g., Criminal Justice Act 2017 [31], NIS2-Directive [13], etc., to protect critical data and provide a path for legal recourse in the event of a breach.
(iii) Compliance with GDPR [32] with a plan to review several identified areas for further assessment and potential remediation.
(iv) Compliance with NIST CSF with a number of focus areas identified that would strengthen Traction Plc's security posture.
(v) A cyber-resilience strategy was developed to ensure that Traction Plc. can continue to operate and deliver products despite cyber-incidents.
(vi) A robust and proven incident response plan to enable Traction Plc. to react to and rapidly recover from a cyber-attack.
(vii) Cyber-auditing to provide assurance that cyber-risk processes and standards are in place and functioning effectively. Auditing will identify any potential security weaknesses that need to be strengthened and will provide assurance that Traction Plc. is compliant with the relevant cyber-laws, including GDPR, in the form of a SOC2 report.

The EU Cybersecurity Resilience Act 2022 is a proposal for a regulation that will ensure the development of digital products, such as hardware and software. The Act will also place an onus on consumers to assess and choose products that meet their security requirements and to ensure that those products are kept secured from cyber-threats for their lifecycle, in line with manufacturer recommendations e.g., hardening, secure firewall configurations, patched up to date, etc. This Act aligns with the previously mentioned cyber, legal, and regulatory standards and sets the tone for building a mature cybersecurity posture.

As a manufacturing company, Traction Plc. relies heavily on technology such as network interfaces, microcontrollers, industrial firewalls, computational resources, operating systems, etc. and will need to comply with these Acts. They will be subject to compulsory external audits to ensure compliance with standards. Based on the recommendations made in this chapter, Traction Plc. has good security and processes in place, but to ensure compliance with the Act, a risk assessment would need to be carried out and any further areas for improvement identified and addressed.

4.7 Conclusion and Future Directions

This chapter gives a high-level overview of the security posture of a use-case manufacturing company. It introduces and implements the authors' designed "CYBER INTEL" (CYBERsecurIty staNdards, risk assessment, Threat Intelligence, Legal, and rEgulatory) framework, which considers the cyber-threat landscape and common attack vectors that ICS networks face and touches on the risk and compliance frameworks and standards, together with cyber-laws that are in place to protect a company's critical assets. It provides a roadmap for developing a strong cyber-resilience strategy and also considers appropriate auditing standards in place for providing assurance over the correct implementation of appropriate security standards and compliance with required laws and regulations. While Traction Plc. has strong foundational security practices in place to address cyber-risk, there are opportunities to reinforce that position and better prepare the company for inevitable cyber-attacks and how best to respond to them to limit their impact. To ensure a return on cybersecurity investment is achieved, it is key that controls, compliance, and support for continued security awareness training are embedded into the company's culture. Cybersecurity and data protection laws that have been enacted in Ireland are pertinent in the battle against cybercrime because they have financial as well as legal consequences. Ultimately, one of the key overall takeaways from this chapter is the need for companies to develop strong and achievable disaster recovery and business continuity plans, which are regularly tested and continuously updated, to allow a company to continue operations and recover from inevitable cyber-attacks which is the core definition of cyber-resilience. Looking toward the future that relies on the digital economy, digital passports, and digital transformation, a world where everything depends on data, cybersecurity would be of utmost importance. The implications and impact of cyber-risk associated with the emerging technologies (i.e., Artificial Intelligence, Quantum Computing, 6G, etc.) used in digital infrastructures would be hard to assess as the technologies have not been fully realized yet and would be susceptible to the novel cyber-threat landscape. The standards for these emerging technologies are still under development, leaving a wide gap open for malicious exploitation. Building and sustaining cyber-resilience in critical infrastructures, industry, and the economy will be the biggest challenge of the future, and it will become crucial to develop new standards and frameworks and build essential skills across these emerging fields. Even in the future, the authors' designed CYBER

INTEL framework will stay intact and provide a roadmap for identifying, aligning, and implementing different cyber, legal, and regulatory standards for building cyber-resilience within the environment.

References

1. Dhirani LL, Armstrong E, Newe T (2021) Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors (Basel, Switzerland) 21 (11):3901. doi:https://doi.org/10.3390/s21113901
2. Worldwide semiconductor industry capital spending will decline by 47.9 percent to $22.9 billion in 2009 – Gartner (2010). Microelectronics International 27 (1). doi:https://doi.org/10.1108/mi.2010.21827aab.004
3. Jenkinson A (2022) US State Attacks and the Continued Oversight of Security. Ransomware and Cybercrime. CRC Press. doi:https://doi.org/10.1201/9781003278214-17
4. Dhirani LL, Newe T (2020) Hybrid Cloud SLAs for Industry 4.0: Bridging the Gap. Annals of Emerging Technologies in Computing 4 (5):41–60. doi:https://doi.org/10.33166/aetic.2020.05.003
5. Chiara PG (2022) The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. International Cybersecurity Law Review 3 (2):255–272. doi:https://doi.org/10.1365/s43439-022-00067-6
6. Burri M, Zihlmann Z (2023) The EU Cyber Resilience Act – An appraisal and contextualization. EuZ – Zeitschrift für Europarecht. doi:https://doi.org/10.36862/eiz-euz015
7. Ashkenazi A (2022) Cyber Diplomacy 3.0 - "Agile Diplomacy" to Promote Security and Innovation. International Journal of Cyber Diplomacy 3:81–96. doi:https://doi.org/10.54852/ijcd.v3y202209
8. Dhirani LL, Mukhtiar N, Chowdhry BS, Newe T (2023) Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors (Basel, Switzerland) 23 (3):1151. doi:https://doi.org/10.3390/s23031151
9. Embroker (2023) Must-Know Cyber Attack Statistics and Trends. www.embroker.com/blog/cyber-attack-statistics. 2023
10. Anwar RW, Bakhtiari M, Zainal A, Qureshi KN (2016) Wireless sensor network performance analysis and effect of blackhole and sinkhole attacks. Jurnal Teknologi 78 (4–3)
11. Kashif Naseer Qureshi AA, Raja Waseem Anwar, Shahid Nazir Bhati, and Gwanggil Jeon (2021) Fully Integrated Data Communication Framework by Using Visualization Augmented Reality for Internet of Things Networks. Big Data 9 (4):253–264. doi:https://doi.org/10.1089/big.2020.0282
12. Lan L, Bai J, Chen X (2020) Overview of Enterprise IoT Security System based on Edge Computing. Paper presented at the Proceedings of the 5th International Conference on Internet of Things, Big Data and Security,
13. Qureshi KN, Rana SS, Ahmed A, Jeon G (2020) A novel and secure attacks detection framework for smart cities industrial internet of things. Sustainable Cities and Society 61:102343. doi:https://doi.org/10.1016/j.scs.2020.102343
14. Lohrmann D, Tan S (2021) Cyber Mayday and the Day After: A Leader's Guide to Preparing, Managing, and Recovering from Inevitable Business Disruptions. John Wiley & Sons,
15. Salbert A (2019) Compatibility of Polish Law with EU Law Concerning the Use of Electronic Communications Means for Direct Marketing Purposes. Yearbook of Antitrust and Regulatory Studies (YARS) 12 (19):53–73
16. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (2022). National Institute of Standards and Technology. doi:https://doi.org/10.6028/nist.cswp.10

17. Government and Oireachtas (2018). The Constitution of Ireland. Hart Publishing. doi:https://doi.org/10.5040/9781509903467.ch-003
18. Dove ES (2018) The EU general data protection regulation: implications for international scientific research in the digital era. Journal of Law, Medicine & Ethics 46 (4):1013–1030
19. Papakonstantinou V (2022) Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? Computer Law & Security Review 44:105653. doi:https://doi.org/10.1016/j.clsr.2022.105653
20. Harding M (2011) The Curious Incident of the Marriage Act (No. 2) 1537 and the Irish Statute Book. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.1742858
21. Avramidou M, Biasin E, Kamenjasevic E, Kun E, Nisevic M Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives. In: Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience, 2023. Steinbeis-Edition,
22. Chiara PG (2022) The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review:1–18
23. Piras L, Al-Obeidallah MG, Pavlidis M, Mouratidis H, Tsohou A, Magkos E, Praitano A (2021) A data scope management service to support privacy by design and GDPR compliance. Journal of Data Intelligence 2 (2):136–165. doi:https://doi.org/10.26421/jdi2.2-3
24. Maclean D (2017) The NIST risk management framework: Problems and recommendations. Cyber Security: A Peer-Reviewed Journal 1 (3):207–217
25. The Top 20 Cyberattacks on Industrial Control Systems (White Paper). (Ginter A (2019)). waterfall-security.com/20-attacks/. Accessed Accessed 7 Mar 2023
26. Cichonski P, Millar T, Grance T, Scarfone K (2012) Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. doi:https://doi.org/10.6028/nist.sp.800-61r2
27. How to Design a Cyber Incident Response Plan for Your Business Embroker. (2022). www.embroker.com/blog/cyber-incident-response-plan. Accessed 18 Mar 2023
28. Davis RE (2021) Cyber Security Governance Audit. Auditing Information and Cyber Security Governance. CRC Press. doi:https://doi.org/10.1201/9781003099673-8
29. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R (2021) Developing Cyber-Resilient Systems. National Institute of Standards and Technology. doi:https://doi.org/10.6028/nist.sp.800-160v2r1