Cyber Security Policy

v2.1

Public

Contents

Introduction

Cyber security at Maersk is about constantly reviewing vulnerabilities, likelihoods and impacts and proactively developing and maintaining mitigating actions. The level to which you want to reduce the Risk is determined by your risk appetite. It may well be that many vulnerabilities are so unlikely to be exploited successfully that you decide to tolerate them and manage the impact.

The Maersk Cyber Security Senior Management Team are committed to using these measures to drive the continual improvement of all Cyber Security activities, functions, and management systems.

This Cyber Security Policy document communicates the principles for the management of cyber security across Maersk and the basis for the organisation and operation of Cyber Security activities and functions.

The Maersk Cyber Strategy

The cyber threat to global supply chains continues to accelerate and a sophisticated criminal eco-system has emerged, where cyber-crime is now big business. We can see this ourselves in the incidents we manage and through our use of the Dark Web to augment our intelligence feeds. Our customers can too, all too often because they are on the receiving end of disruption caused by companies in the logistics sector falling victim to Ransomware.

As the global integrator of container logistics, our customers increasingly value cyber security as a differentiator. They need to be able to trust Maersk with their data and be able to rely on our cyber resilience. This is why we now employ over 300 highly skilled and experienced Maersk Cyber Security colleagues and why there has been considerable investment in cyber security technology since the 2017 NotPetya incident, which originated in Ukraine and affected Maersk alongside many global companies. Currently, our defences process 30 billion cyber events a week, but the automation we have implemented so far means that our human defenders only need to focus on processing 1,000-2,000 cyber incidents a week. This results in Maersk on average experiencing one incident a day globally that could have a harmful impact, which Cyber Security then locally contain and eradicate so business can carry on without wider interruption. This is what it means to be cyber resilient.

In 2022 we worked with insurance industry experts to assess our progress to date and Maersk's current exposure to a NotPetya level of impact. The conclusion of the analysis is that the probability of a similar sized impact in terms of direct costs associated with business interruption following system outage, data restoration, liability for data breaches, data asset losses, ransomware, and fines is now a once in 100 years event at our current level of capability. However, the risk of a successful cyber-attack causing major operational disruption and/or data breach to Maersk and/or its third parties and supply chain continues to be managed by the CISO, owned by the CTIO and overseen by the Audit Committee on behalf of the Board of Directors, as it is still a risk whose likelihood the Board want to reduce further. As a consequence, the aim of our Maersk cyber strategy is to continue to reduce the likelihood of the risk of a major cyber-attack to the point where it ceases to be material to the Board.

The way we are implementing the strategy is to nest it within the CTIO's Technology Strategy which, in turn, is nested inside the A.P. Moller – Maersk company strategy. Moreover, the resources we employ to achieve the aim are not just the resources of the Cyber Security organisation, but a whole-of-company approach including all A. P. Moller–Maersk group entities, employees, contractors and third parties.

At the core of the cyber strategy are 5 key actions that control the overall risk. These are:

- An operating model based on the internationally recognised Cybersecurity Framework of the US National Institute of Standards and Technology (NIST), with Continuous Improvement in the Identify, Protect, Detect, Respond and Recover functions and regular independent benchmarking of our maturity across those functions against leaders in the Transport & Logistics sector.
- Continued investment in cyber security capabilities (people, process and technology) using advanced techniques to model cyber risk and quantify impact in financial terms to prioritise investment decisions, with implementation delivered through our own Agile engineering teams.

- Timely management of patching of vulnerabilities in the A.P. Moller – Maersk estate so that issues do not develop into systemic risks.
- Sustainment of operational excellence in our organic, 24/7, intelligence-led, Global Cyber Defence Centre, providing outstanding levels of global visibility and response that means customers can fully rely on Maersk as their partner.
- Maintenance of 3 lines of defence in our assurance and compliance regime: a First Line of Defence that includes automated checking of logs from Maersk software applications; a Second Line of Defence that includes our own internal assurance team measuring deviation against cyber standards, augmented by PwC who assist with our SOC2 Type2 assessment and certifications and independently assess our Cyber Security maturity; and Third Line of Defence operated by Group Internal Audit and external auditors.

Scope

This cyber security policy applies to:

- all A. P. Moller–Maersk (APMM) Group entities, employees, contractors and third parties
- all information, IT systems, Operational Technology ("OT"), Industrial Control Systems ("ICS"), and Internet of Things (IoT)\Industrial Internet of Things (IIoT) devices

For further information, please contact Cyber Security department.

Policy Requirements

Cyber Security Governance

1.1 A Chief Information Security Officer (CISO) is appointed and ensures that all roles and responsibilities for the Maersk Cyber Security department are defined, allocated and resourced by suitably skilled individuals.

1.2 The interaction between the Cyber Security organisation and other business and Technology functions is defined and understood, with business representatives identified to maintain the operational effectiveness of the security control environment.

1.3 A cyber strategy is defined and communicated, that sets the vision and objectives for cyber security at Maersk and its continual alignment to strategic business objectives. The strategy informs cyber policy and standards, cyber security operating models, resource allocation and processes that enable the operation of cyber services.

1.4 The cyber security policy and standards are continually improved to ensure alignment with the cyber strategy and communicate the agreed security baseline against which cyber risk can be identified and managed.

1.5 Where possible, staff are contractually required to be aware of and abide by Maersk Cyber Security Policy.

1.6 Security governance forums are established to manage cyber security risk, identify, and improve security services delivered to the business and coordinate responses to major security incidents.

1.7 Maersk endeavour to comply with legal, regulatory, and contractual requirements. Local laws and regulations take precedent in cases where Maersk Cyber Security Policy conflicts with them.

1.8 Cyber security risk is identified, assessed, and managed across the enterprise, including centrally managed functions, third-parties, subsidiaries, joint ventures, platforms, disconnected brands, and as part of merger, acquisition, or divestment activity.

1.9 The Cyber Security department lead the cyber risk management activities and involve business managers to identify, assess, manage, and treat information risks within their areas of responsibility.

1.10 Risk assessments are conducted as part of project and change management and include the potential business impact of the risk in terms of compromise to the confidentiality, integrity, availability or safety of the asset. The assessment includes the likelihood of the impact occurring.

1.11 The implementation and effectiveness of agreed risk mitigation is monitored, measured, and reported to ensure that risks are being managed and reduced as intended.

1.12 Security testing is conducted to identify vulnerabilities in people, processes or technology that could lead to a compromise.

1.13 When adopting cloud services, appropriate governance processes are established to ensure cyber risks are managed and responsibility for the implementation of suitable security controls is assigned and agreed.

Asset Identification and Inventory Management

2.1 All information and technology assets are identified, approved, recorded, and managed. Unauthorised software, hardware, and cloud services must be identified, and approved or removed from use.

2.2 Only trusted, robust, reliable hardware and software is acquired and is checked to determine whether it is suitable for use.

2.3 Details for all approved information and technology assets are recorded, with owners assigned that are responsible and accountable for safeguarding them throughout their lifecycle.

2.4 Technology assets are categorised as either IT, OT or IoT based on documented criteria to allow them to be appropriately managed and protected.

2.5 The criticality of assets is determined and reviewed on a regular basis to ensure that resources can be prioritised.

2.6 All information and technology assets are classified and appropriately labelled in line with relevant legislation, regulation, and the Maersk Information Classification Scheme.

2.7 Systems processing personal data are recorded and assessed to ensure that risks to both the organisation and affected data subjects is understood and controlled, in line with Maersk Rule for Data Privacy Compliance.

2.8 Information retention requirements are understood to ensure that it is only kept by Maersk as long as is necessary to adhere to applicable legal, regulatory, and business expectations.

Supplier Security

3.1 The criticality of external suppliers is established, with consideration for both the criticality of the assets or services they are providing and the number of services that the supplier provides.

3.2 A supplier risk assessment is performed to establish the risks and security requirements of any assets that will be processed or stored by an external supplier.

3.3 Non-disclosure agreements (NDAs) or other legally binding agreements are established prior to the sharing or transfer of confidential information between Maersk and a third-party.

3.4 Supplier cyber security risks are identified and managed throughout the lifecycle of the relationship with the suppler.

3.5 Cyber security and data privacy requirements are defined, agreed, and embedded in contracts with external suppliers.

3.6 Mechanisms are in place to ensure that all suppliers hosting or processing Maersk data protect against unauthorised access, disclosure, modification, or monitoring and in compliance with regulatory requirements (e.g., GDPR, PCI-DSS, etc.).

3.7 Any suppliers developing applications or code on behalf of Maersk are contractually obliged to respect Maersk intellectual property rights and secure development principles.

3.8 Prior to the procurement of IT/OT/IoT equipment or devices from external suppliers the minimum-security measures are established. The suppliers' security posture and the security of the product is assessed for possible risk to the Maersk environment in which

they will be operating.

3.9 Processes are established to ensure that suppliers are able to report in a timely manner any cyber incidents that may adversely affect Maersk assets or services.

3.10 A formal process is established for exiting, terminating, renewing, and renegotiating contracts with external suppliers ensuring all Maersk information is returned in a useable manner or securely disposed of by the external supplier.

Identity and Access Management

4.1 Access to information and technology assets is attributed to an account which can be tracked to an individual whose identity has been formally assured.

4.2 All individuals are accountable for the safeguarding and the appropriate usage of accounts and access that is assigned to them.

4.3 Access to information and technology assets is granted, managed, reviewed and revoked according to defined and implemented access control mechanisms, procedures, and ongoing business needs.

4.4 Privileged access is granted, managed, and monitored with increased control and scrutiny relevant to the risk posed, and only for the time it is required.

4.5 Authentication mechanisms are in place to ensure that only approved users, processes, devices, or networks may connect to Maersk information or technology assets.

4.6 End-user computing devices accessing Maersk corporate networks or resources do so via approved secure services, and it is ensured that appropriate security tooling is installed on these connected devices.

4.7 Authentication mechanisms and credentials are proportionately robust to address the risk related to the assets that they are protecting, and the access levels being requested.

4.8 Robust physical security is established for environments where IT or OT technology infrastructure is housed, or business information is processed, with access only granted to appropriately authorised individuals.

4.9 IoT devices and infrastructure are protected against unauthorised access, with consideration to the differing environments to which they may operate and the limitations against implementing traditional physical protections.

Awareness and Training

5.1 Awareness and training is delivered to ensure that all staff are adequately informed in the secure operations of technology and protection of information in relation to current and emerging cyber threats.

5.2 A Cyber Security Acceptable Use Policy is distributed to all users, which provides mandatory requirements for acceptable use of Maersk technology and information.

5.3 Role-based security training is provided to all individuals responsible for the operation of security processes, tools, and technology in the protection of Maersk assets.

Asset Change Control and Maintenance

6.1 Configuration Management is used to understand and record the hardware, software and network components that underpin systems supporting business applications and information.

6.2 Change and release management processes are enforced to ensure changes are risk assessed, tested, recorded, approved, and implemented securely.

6.3 Hardware, software, and network maintenance is managed and carried out by authorised and appropriately trained personnel, using secure methods and tools.

6.4 Any third parties carrying out maintenance activity on Maersk systems or networks, are securely onboarded and agree to the scope of maintenance activity they are expected to perform.

Data Protection and Encryption

7.1 A secure network architecture is established and maintained to ensure that all traffic flow requirements are understood and managed to minimize the risk of a cyber-attack or data breach.

7.2 Direct connections from external networks to the Maersk internal corporate network are not permitted. Connections from external networks are terminated on a device within an external DMZ, owned, controlled, and managed by Maersk.

7.3 Networks are appropriately zoned and segregated with consideration for the business purpose, classification and criticality of the information, information systems and services on the networks.

7.4 Production environments are segregated from development and test environments to protect against unauthorised access to business information, and unauthorised changes to business systems.

7.5 Throughout their lifecycle, information and technology assets are protected and handled to ensure against unauthorised access, disclosure, or modification, and meet availability and safety requirements in accordance with contractual obligations and applicable legislation.

7.6 Information, whether in transit or at rest, is appropriately encrypted in accordance with its classification level, using suitable cryptographic algorithms and protocols.

7.7 Cryptographic key management is established to ensure encryption keys are protected against unauthorised access, copying, disclosure and malicious or accidental destruction.

7.8 Processes are established, governing the use of removable media devices to prevent unauthorised access as well as any loss or theft of the devices and the information that is held on them.

7.9 The disposal of information and technology assets (including backups) is securely undertaken in accordance with their classification, using approved methods for destruction.

System Hardening

8.1 Systems, applications, and networks are designed and configured in line with established security architecture and validated secure baseline configurations to ensure that they meet their intended functional and security requirements.

8.2 Information systems are developed following a Software Development Lifecycle (SDLC) that incorporates Secure by Design (SBD) principles at every stage to ensure that cyber risks are identified and mitigated.

8.3 Privacy by Design and Default (PbDD) principles are applied to all applications and systems that process personally identifiable information (PII).

8.4 Any software used or distributed by the organisation is approved, deployed securely and in accordance with contract agreements and copyright restrictions.

8.5 Technical vulnerabilities in all applications, middleware, infrastructure components and operating systems are identified, remediated, and reported upon, with prioritisation based on criticality and likelihood of exploitation.

Security Monitoring

9.1 Threat intelligence and advisory services are utilised to collect and assess threats and vulnerabilities, and to prioritise protection or remediation activities.

9.2 Security related events are logged, stored, and retained in approved locations and protected against unauthorised change or deletion in accordance with local legislation or regulation.

9.3 All system clocks are synchronised with an authoritative trusted time source to ensure accurate event logging.

9.4 Where possible, security event logs are centrally collated in a manner that allows for correlation and analysis.

9.5 Security events are correlated with threat intelligence and other relevant security monitoring sources to identify suspicious, inappropriate, unusual, or malevolent activity and trigger appropriate security incident response activities.

9.6 Automated and intelligent tooling is deployed to detect and protect against malicious activity such as email spam, network intrusions, malware, and malicious or unauthorised code.

9.7 Physical security mechanisms are placed on the perimeter of Maersk sites and around high-risk areas in order to detect attempted unauthorised physical access to assets.

Security Incident Response

10.1 A Cyber Incident Response Plan (CIRP) and set of procedures is established that enable all applicable teams to work in a coordinated way to manage cyber incidents and recover effectively.

10.2 Cyber security incidents are identified and reported:

- when security policies are breached
- in case of a failure of a security measure that detrimentally affects or attempts to affect the confidentiality, integrity, availability and/or safety of business information or systems or

- when unusual behaviour is detected through protective monitoring

10.3 Cyber security incidents are categorised based on their impact on Maersk's critical business processes and in line with pre-defined criteria, which drive the appropriate response to the incident.

10.4 Cyber security incidents are analysed, contained, and eradicated in coordination between the Cyber Security Operations department, appropriate internal teams, and external service providers.

10.5 Maersk maintain a capability to perform enterprise and endpoint forensics in order to support incident response processes and identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

10.6 Maersk adhere to regulatory and contractual obligations that require accurate and timely reporting of breaches to regulators or third parties.

10.7 Knowledge gained from analysing and resolving security incidents is used to extract lessons learned and initiate activity to reduce the likelihood or impact of a reoccurrence of the same incident in the future.

10.8 The incident response plan and procedures are regularly tested and/or exercised to determine the incident response effectiveness.

Disaster Recovery

11.1 There is an information and technology resilience strategy, that aligns to the organisation's business continuity objectives, and ensures that recovery requirements for all assets are identified and can be achieved.

11.2 Recovery plans are developed, documented, maintained, communicated, and regularly tested to support all information and technology services related to business-critical assets.

11.3 Recovery plans and incident response plans are aligned to the critical incident management process, with clear links to the Major Incident Management process.

11.4 Recovery plans are coordinated across all appropriate internal and external service providers to ensure that business continuity requirements can be satisfied.

11.5 Continuity planning ensures that necessary capacity and alternate services for information processing, telecommunications, and environmental support exists in the event of a total loss of a primary service or site.

11.6 All business information has appropriate retention, backup and retrieval processes and mechanisms in place, with backups of information and software performed on a regular basis and according to an agreed schedule.

11.7 Backups are protected from loss, damage, unauthorised access, or modification.

11.8 The recovery of data from backup media is regularly tested to ensure reliability, availability and integrity can be assured in the case of a recovery event.

Review and Monitoring

All cyber security policies are reviewed at least annually or when there has been a significant change to business operations or the cyber strategy.

The owner of the cyber security policies is responsible for ensuring that these reviews take place.

Comply or Explain

Maersk cyber security policy and standards contain mandatory rules that must be adhered to by all Maersk functions. Non-compliance must be reported and follow the Risk Management process.

Enforcement

Breaches of the Maersk cyber security policies may lead to disciplinary sanction.

Version Control

Version	Date	Author	Description
1.0	20 Nov 2018	CSP-GRC	Creation of a new policy; approved by Policy Approval Board on 15th November 2018
1.1	10 Jan 2019	CSP-GRC	Updated the terminology from 'Information Security' to 'Cyber Security'
1.1	10 Jan 2020	CSP-GRC	Annual Review – No updates
1.1	11 Jan 2021	CSP-GRC	Annual Review – No updates
2.0	24 Nov 2021	Cyber Regulation and Policy	Major update to simplify layout, reflect Cyber Strategy, and clearer link to Cyber Standards.
2.1	13 Oct 2023	Cyber Regulation and Policy	Updated Cyber Strategy Added considerations for IoT and safety Other amendments in line with Standard updates