Critical Infrastructure OT Cybersecurity

Regulation Reference Guide

Updated
October 14, 2024

Contents

About this Guide

As public sector agencies respond to the increase in both the sophistication and incidence of cyberattacks on critical infrastructure, there is a need to track regulates and government mandates. The purpose of this guide is to provide a summary of the most important regulations that relate to Critical Infrastructure OT Cybersecurity in major industrial economies.

This document should be used for references purposes and not as a primary source of regulatory information.

OT Cyber Guidelines

NIST IR 8228 (US)

NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST SP 800-82r3 is a foundational guide for securing OT environments, including ICS, SCADA, and distributed control systems. It emphasizes the protection of physical processes from cyber threats that impact critical infrastructure, addressing both external and internal risks.

Regulatory Body

National Institute of Standards and Technology (US Department of Commerce)

What's Involved

- **OT Security Guidance:** Provides tailored security measures for OT systems, addressing their unique performance, reliability, and safety needs. It focuses on systems that interact with the physical environment.
- **Risk Management Framework:** Emphasizes a risk management approach specific to OT systems, focusing on identifying, assessing, and mitigating threats to operational integrity.
- **Incident Detection and Response:** Advocates for real-time monitoring, anomaly detection, and swift response to incidents to ensure system resilience and recovery.
- **Defense-in-Depth Approach:** Recommends layered security strategies, including network segmentation, access control, and continuous monitoring to protect against cyber threats.

Applicable Sectors

Applicable across sectors that rely on OT, including:

- Energy
- Water and Wastewater Systems
- Manufacturing
- Transportation
- Healthcare
- Other critical infrastructure sectors

Reporting Requirements

Does not outline specific incident reporting requirements.

Penalties for Non-Compliance

Serves as a set of best practices and not impose penalties.

References to Process-Oriented OT Cybersecurity

Emphasizes security measures for OT systems that manage critical processes at various levels, including Level 0 systems (Purdue model), which involve direct control over physical processes. It highlights the importance of securing these systems against threats that could manipulate or disrupt critical physical operations.

As stated in 5.3.6. Field I/O (Purdue Level 0) Security Considerations of **NIST.SP.800-82r3**:

Many of the devices and the communication protocols at the Field I/O level (Purdue Level 0) (e.g., sensors, actuators) cannot be authenticated. Without authentication, there is the potential to replay, modify, or spoof data. Organizations should make a risk-based decision to decide where within the OT system (e.g., the most critical process) the use of mitigating security controls (e.g., digital twins, separate Field I/O monitoring network) should be implemented to detect incorrect data.

Additional Resources:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

OT Cybersecurity Masterplan 2024 (Singapore)

The OT Cybersecurity Masterplan 2024 is a national strategy developed by the Cyber Security Agency of Singapore (CSA). This blueprint aims to secure critical infrastructure (CI) sectors and strengthen the overall OT landscape in Singapore. It focuses on addressing evolving OT cyber threats by improving technical capabilities, boosting the workforce's expertise, and fostering collaboration between public and private sectors.

Regulatory Body

Cyber Security Agency of Singapore (CSA)

What's Involved

- **Enhanced Technical Capabilities**: Focuses on improving cybersecurity technologies and resilience to emerging threats in OT systems, especially with the integration of IoT, edge computing, and other new technologies.
- **Workforce Development:** Establishes programs to build a robust OT cybersecurity talent pipeline, ensuring that Singapore has a competent workforce capable of responding to advanced cyber threats.
- **Collaboration and Threat Intelligence:** Enhances information-sharing mechanisms via the OT Information Sharing and Analysis Center (OT-ISAC) to create a comprehensive threat intelligence ecosystem and ensure swift responses to cyber threats.
- **Supply Chain Risk Management:** Introduces a data-driven model to monitor cyber risks within the OT supply chain, applicable to both CII and non-CII sectors, ensuring accurate risk assessments and vendor analysis.

Applicable Sectors

Applicable to sectors heavily reliant on OT systems, including:

- Energy
- Water
- Transportation
- Healthcare
- Telecommunications
- Manufacturing and Industrial sectors

Reporting Requirements

Key reporting requirements include:

- **Mandatory Incident Reporting:** CI operators must report significant cybersecurity incidents to the CSA within specific timelines to ensure timely responses and damage mitigation.

- **Threat Intelligence Sharing:** CI operators are required to participate in the OT Information Sharing and Analysis Center (OT-ISAC), which facilitates the exchange of cybersecurity intelligence and incident information to bolster sector-wide defenses.

Penalties for Non-Compliance

Non-compliance with the Cybersecurity Act and the Masterplan's provisions may result in fines, regulatory actions, or restrictions on the operation of critical infrastructure, depending on the severity of the violation.

References to Process-Oriented OT Cyber Security

The Masterplan advocates for a holistic approach to OT cybersecurity, which implicitly includes securing the process level of OT environments. It emphasizes protecting physical processes that are essential for CI, stressing the importance of implementing secure communication, continuous monitoring, and anomaly detection to safeguard against attacks that could disrupt critical services like power and water distribution.

Additional Resources:

https://www.csa.gov.sg/Tips-Resource/publications/2024/operational-technology-cybersecurity-masterplan-2024

Water Sector Cybersecurity Program (US)

EPA
OFFICE OF GROUND WATER AND DRINKING WATER
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Water Security is National Security

The EPA's Water Sector Cybersecurity Program provides guidance, resources, and tools to help water and wastewater utilities enhance their cybersecurity posture. It is part of the EPA's broader efforts to protect critical water infrastructure from cyber threats.

Regulatory Body

Environmental Protection Agency

What's Involved

The program supports utilities by offering technical assistance, developing best practices, and promoting cybersecurity awareness. The EPA collaborates with other federal agencies and industry partners to provide up-to-date information and resources tailored to the specific needs of the water sector. Major elements include:

- **Cybersecurity Incident Action Checklist:** A step-by-step guide for utilities to prepare for and respond to cybersecurity incidents.
- **Technical Assistance:** Direct support to utilities in identifying vulnerabilities and implementing cybersecurity measures.
- **Partnerships:** Works with organizations like the Department of Homeland Security (DHS) and the Water Sector Coordinating Council to improve cybersecurity across the sector.

Applicable Sectors

Applicable to the following sector:

- Water and wastewater utilities

Reporting Requirements

The program does not impose specific reporting requirements, but it encourages utilities to document cybersecurity incidents and share relevant information with the EPA and other federal agencies to improve collective security efforts.

Penalties for Non-Compliance

There are no direct penalties associated with the program itself, as it is primarily a resource and guidance initiative.

References to Process-Oriented OT Cyber Security

The Water Sector Cybersecurity Program highlights the importance of safeguarding OT systems, which are critical for managing water treatment and distribution processes. The program encourages utilities to protect control systems and physical processes that ensure the safe and reliable operation of water services.

Additional Resources:

https://www.epa.gov/climate-change-water-sector/water-and-wastewater-systems-sector-cybersecurity

Regulations and Standards

ISA/IEC 62443 Standard (International)

A series of standards developed to secure Industrial Automation and Control Systems (IACS) across various sectors. These standards provide a comprehensive approach to cybersecurity, addressing both organizational processes and technical security measures.

Regulatory Body

International Society of Automation (ISA) and International Electrotechnical Commission (IEC)

What's Involved

- **General Requirements:** Defines fundamental concepts, models, and terminology, providing a framework for securing IACS.
- **Policies and Procedures:** Security policies, roles, and responsibilities, and procedures for implementing and maintaining cybersecurity measures.
- **System Requirements:** Requirements for the design, operation, and maintenance of IACS systems, focusing on protecting against a broad range of threats.
- **Component Requirements:** Defines security requirements for IACS components, such as controllers, field devices, and software applications.
- **Implementation Guidance:** Guidance on implementing security measures in IACS, including recommendations for designing secure systems and managing vulnerabilities.

Applicable Sectors

Various sectors that rely on IACS including:

- Energy (e.g., power plants)
- Water and wastewater systems
- Oil and gas
- Manufacturing
- Pharmaceuticals
- Transportation
- Building management systems

Reporting Requirements

ISA/IEC 62443 does not mandate external reporting requirements.

Penalties for Non-Compliance

ISA/IEC 62443 does not prescribe penalties.

References to Process Oriented OT Cyber Security

ISA/IEC 62443 is essential as it refers to the physical process and the sensors/actuators that interact directly with the physical world. The standard emphasizes that protecting these components is critical because any vulnerability at this level can have a direct and immediate impact on the safety and reliability of the entire industrial system.

Additional Resources:

https://isagca.org/isa-iec-62443-standards

ISO/IEC 27019 Standard (International)

Part of the ISO/IEC 27000 family of standards, specifically tailored for the energy utility sector, focusing on unique industry requirements, including generation, transmission, distribution, and supply of energy.

Regulatory Body

International Society of Automation (ISA) and International Electrotechnical Commission (IEC)

What's Involved

- **Information Security Controls:** Identifies and assesses risks specific to the energy sector, provides guidance on implementing security controls to mitigate identified risks and focuses on reliability and safety issues.
- **Best Practices:** Provides best practices on Access Management, Incident Management and Business Continuity.

Applicable Sectors

Applies to the following sector:

Energy: Organizations involved in power generation (e.g., nuclear, hydro, solar), transmission, distribution, and supply.

Reporting Requirements

While ISO/IEC 27019 does not mandate external reporting requirements.

Penalties for Non-Compliance

ISO/IEC 27019 does not prescribe penalties.

References to Process Oriented OT Cyber Security

Not specific reference to Process Oriented but aligns with NIST Cybersecurity Framework.

Additional Resources:

https://www.iso.org/standard/68091.html

Cybersecurity Code of Practice for Critical Information Infrastructure (Singapore)

The Cybersecurity Code of Practice (CCoP) for Critical Information Infrastructure (CII) is a mandatory regulatory framework established by the Cyber Security Agency of Singapore (CSA). It defines the necessary cybersecurity measures that CII operators must implement to safeguard essential services from cyber threats. The Code plays a vital role in ensuring that organizations responsible for CII take the necessary steps to secure their OT systems, infrastructure, and processes.

Regulatory Body

Cyber Security Agency of Singapore (CSA)

What's Involved

- **Cybersecurity Risk Management:** CII operators are required to conduct regular cybersecurity risk assessments to identify vulnerabilities in OT systems and mitigate potential risks.
- **Incident Response Planning:** Organizations must have well-defined incident response procedures to ensure quick and effective action during a cybersecurity event.
- **Continuous Monitoring:** The Code emphasizes the importance of monitoring OT systems for anomalies and threats in real time to enable proactive defenses.
- **Security Policies and Processes:** CII organizations must establish comprehensive security policies and standard operating procedures to ensure consistency in cybersecurity practices.
- **Supply Chain Security:** CII operators must manage and monitor the security of their supply chain to prevent risks from third-party vendors and contractors.
- **Penetration Testing:** Regular testing of OT systems to identify and address weaknesses is mandated by the Code.

Applicable Sectors

Applies to all sectors identified as essential services, including:

- Energy
- Water and wastewater systems
- Transportation
- Healthcare
- Telecommunications
- Financial Services

Reporting Requirements

CII operators must report cybersecurity incidents to the **Cyber Security Agency of Singapore (CSA)** in a timely manner. This enables prompt incident handling and response, reducing the potential damage caused by cyber incidents.

Penalties for Non-Compliance

Failure to comply can result in severe penalties, including fines, suspension of operations, and other enforcement actions depending on the severity of the non-compliance and its impact on critical infrastructure.

References to Process-Oriented OT Cyber Security

Emphasizes the protection of **process-level (Level Zero)** operations. The Code stresses the importance of securing physical processes, sensors, and control systems to prevent unauthorized access and ensure the integrity of data flowing from OT systems.

Additional Resources:

https://www.csa.gov.sg/legislation/Codes-of-Practice

TSA Security Directive Pipeline 2021-02D

The TSA's Security Directive Pipeline 2021-02D is designed to strengthen the cybersecurity posture of critical pipeline operators. The directive mandates real-time reporting of cyber incidents, annual vulnerability assessments, and the implementation of cybersecurity measures to protect critical operational technology (OT) systems. With an emphasis on Incident Response, it seeks to prevent disruptions to physical pipeline operations and improve resilience to cyberattacks, making compliance crucial for maintaining both operational integrity and national security.

Regulatory Body

Transportation Security Administration (US Department of Homeland Security)

What's Involved

Critical Cyber Systems Identification: Operators must identify systems vital to pipeline cybersecurity and create an actionable cybersecurity plan.

Incident Response: Requires operators to implement incident response plans. The directive states: "Incorporate incident response, mitigation, and forensic analysis procedures into your OT systems to ensure threats are addressed in real-time."

Vulnerability Assessments: Operators must conduct annual cybersecurity vulnerability assessments and implement corrective actions.

Cybersecurity Measures: Measures include access controls, system monitoring, and real-time incident response.

Incident Reporting: Operators must report cybersecurity incidents to CISA within 24 hours of discovery and provide follow-up reports as required.

Applicable Sectors

- Energy (pipeline operators)

Reporting Requirements

Real-time reporting of incidents to CISA within **24 hours**.

Operators must also submit an **annual** report of cybersecurity incidents.

Penalties for Non-Compliance

Operators may face financial penalties, which are dependent on the severity of non-compliance. Potential operational restrictions include the suspension of operations if key security measures are not in place. Other enforcement actions may be taken by the TSA to ensure compliance.

References to Process-Oriented OT Cyber Security

The directive is designed to protect OT systems that control physical processes within pipelines. It emphasizes cybersecurity measures that detect and prevent attacks targeting the critical infrastructure of pipelines.

Additional Resources:

https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit

Legislation

Cyber Incident Reporting for Critical Infrastructure Act (US)

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), passed in 2022 and implemented in 2024, is a federal regulation that mandates timely reporting of cybersecurity incidents affecting critical infrastructure sectors.

Regulatory Body

Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS)

What's Involved

- **Mandatory Incident Reporting**: Organizations operating within critical infrastructure sectors, including water and wastewater systems, must report any significant cybersecurity incidents to CISA within **72 hours** of detection.
- **Ransomware Payment Reporting**: In addition to cyber incidents, organizations must also report any **ransomware payments** made in response to cyberattacks within **24 hours** of payment. This aims to improve the understanding and response to ransomware threats across critical sectors.
- **Incident Management**: CIRCIA empowers CISA to analyze data from these reports to identify trends, provide early warnings, and help mitigate future threats.

Applicable Sectors

Applies to all critical infrastructure sectors, including:

- Water and wastewater systems
- Energy
- Healthcare
- Transportation
- Financial services

Reporting Requirements

CIRCIA imposes strict reporting deadlines:

- **Cyber Incident Reporting**: Must report within **72 hours** of discovering a significant cybersecurity incident affecting critical infrastructure.
- **Ransomware Payments**: Must report within **24 hours** of making any ransomware payments.

These reports should include details about the nature of the incident, its potential impact, and any actions taken to mitigate the risks.

Penalties for Non-Compliance

While **CIRCIA** does not specify penalties for non-compliance, failure to report incidents or ransomware payments could result in **regulatory actions** by DHS, including potential fines or sanctions.

References to Process-Oriented OT Cybersecurity

CIRCIA's focus on critical infrastructure protection extends to OT systems, particularly those controlling physical processes like water treatment plants and energy systems. Continuous monitoring of cyber threats to OT environments, including process-level operations, is encouraged under the act, ensuring protection against incidents that could disrupt critical services.

Additional Resources:

https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf

EU AI Act (Artificial Intelligence Act) Legislation (EU)

The EU AI Act is the European Union's first comprehensive regulatory framework for artificial intelligence. It aims to ensure the safe and ethical use of AI across various sectors, with specific requirements for high-risk AI systems, including those integrated into OT systems within critical infrastructure.

Regulatory Body

European Commission

What's Involved

- **General Requirements**: The AI Act categorizes AI systems based on risk levels, with high-risk systems, particularly in critical infrastructure, subject to strict regulation.
- **Policies and Procedures**: Requires organizations to implement risk management policies, data governance, and accountability measures for AI systems.
- **System Requirements**: Focuses on ensuring that AI systems used in critical infrastructure are transparent, explainable, and free from bias.
- **Component Requirements**: Specifies the security, reliability, and transparency requirements for AI components used within OT systems.
- **Implementation Guidance**: Provides detailed guidelines on implementing AI systems in critical infrastructure, including risk assessment, data management, and compliance with the Act's requirements.

Applicable Sectors

Applies to the following sectors:

- Energy
- Water and wastewater
- Transportation
- Healthcare
- Digital Infrastructure

Reporting Requirements

Organizations using high-risk AI systems must maintain detailed records of their AI applications and report significant incidents to relevant authorities.

Penalties for Non-Compliance

Penalties for non-compliance can include fines up to **6% of global annual turnover**, highlighting the importance of adhering to the Act’s requirements.

References to Process-Oriented OT Cybersecurity

The AI Act does not explicitly reference Level Zero but underscores the importance of securing AI components that interact with OT processes, ensuring they do not introduce vulnerabilities at the foundational process level. The Act emphasizes that "high-risk AI systems deployed in critical infrastructure must be designed with robust security measures to prevent any disruption to essential services."

Additional Resources:

https://artificialintelligenceact.eu/

Network and Information Security Directive Legislation 2023 (NISD 2) (EU)

Requires critical infrastructure operators to implement thorough Incident Response capabilities. The aim is to ensure that any potential security incident is managed effectively to minimize harm to critical services.

Regulatory Body

European Commission and ENISA (European Union Agency for Cybersecurity)

What's Involved

NIS2 mandates comprehensive risk management and cybersecurity measures across critical infrastructure sectors. It emphasizes:

- **Identification of Risks:** Organizations are required to identify and assess risks associated with their OT systems, including SCADA systems, PLCs, and process-level sensors.
- **Protection of Assets:** Like NIST's guidelines, NIS2 emphasizes securing critical assets, advocating for strong authentication, encryption, and real-time monitoring of OT components.
- **Incident Detection and Response**: Organizations must have the capability to detect, respond to, and recover from incidents, aligning with the NIST Cybersecurity Framework's core functions—Identify, Protect, Detect, Respond, and Recover.

Applicable Sectors

Applies to the following sectors:

- Energy (e.g., power grids, nuclear facilities)
- Water and wastewater systems
- Transportation (e.g., rail networks, air traffic control)
- Healthcare (e.g., hospitals, medical devices)
- Digital Infrastructure (e.g., data centers, telecom networks)

Reporting Requirements

Reporting requirements are designed to ensure swift communication between affected entities and national authorities. Key reporting obligations include:

- **Initial Reporting:** Organizations must report incidents **within 24 hours** of detecting any security breach that significantly impacts their services. situation.
- **Intermediate Report:** Within **72 hours**, a more detailed report must be submitted. This report should outline the nature of the incident, its origin (if known), and the steps taken to mitigate the impact. It should also include the expected timeline for full-service restoration.

- **Final Report:** After resolving the incident, a final report must be submitted no later than **a month** that includes a full post-incident analysis. This report should detail the cause, the effects on services, and the corrective measures implemented to prevent a recurrence.

Penalties for Non-Compliance

- **Financial Penalties:** Failure to comply with reporting obligations can result in substantial fines, up to **€10 million** or **2% of the total worldwide annual turnover**, whichever is higher.
- **Administrative Sanctions:** Additional sanctions may include corrective orders, temporary bans on activities, or public notices detailing non-compliance.
- **Executive Accountability:** Senior management may be held personally accountable for failures in reporting and managing cybersecurity incidents appropriately.

References to Process Oriented OT Cyber Security

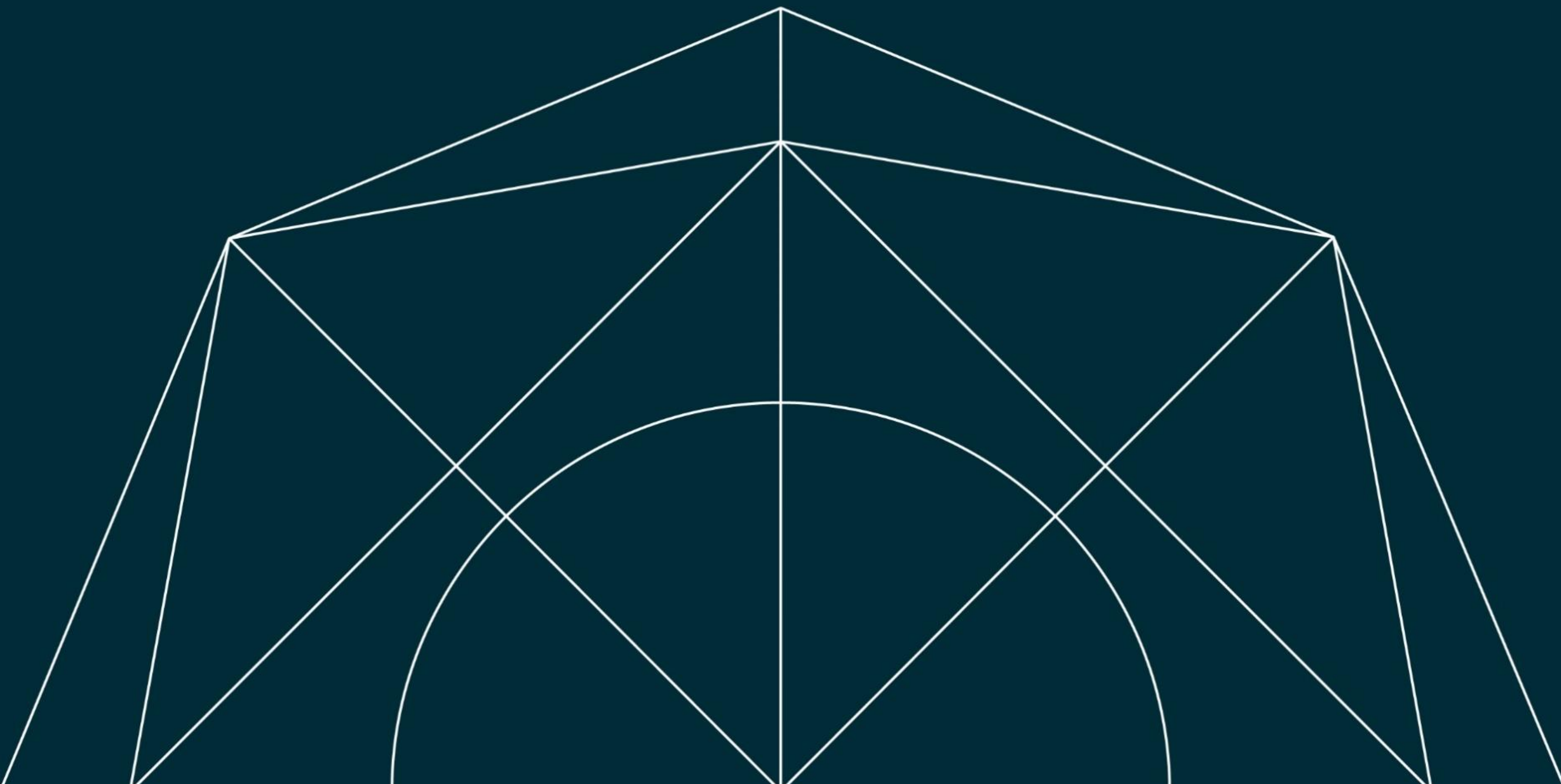
The **NIS2 Directive** emphasizes robust cybersecurity measures for critical infrastructure, including **process-level OT security**. This includes ensuring the safety of physical processes that are central to essential services, such as those managed by **SCADA systems, PLCs**, and sensors.

While NIS2 does not specifically label **Level Zero**, the directive strongly advocates securing critical OT components from disruptions that could affect physical processes, particularly in sectors like energy, water, and transportation. The directive emphasizes **real-time monitoring**, **anomaly detection**, and **strong access controls** to ensure the integrity of these systems.

Additional Resources:

https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Financial Disclosure



Cybersecurity Disclosure Rule (US)

U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV
U.S. Securities and Exchange Commission

2023 rules that require public companies to disclose significant cybersecurity incidents, including those affecting OT which are deemed material to investors.

Regulatory Body

Securities and Exchange Commission (SEC)

What's Involved

- **Form 8-K Reporting:** Reporting of cybersecurity incidents within **four business days of determining the materiality of the event.**
- **Board Oversight Disclosure:** Companies must report how its Boards of Directors oversee cybersecurity risk management.
- **Annual Reporting:** Companies must include a detailed description of their cybersecurity risk management processes in their annual reports (Form 10-K).

Applicable Sectors

This disclosure requirement applies to all publicly traded companies across sectors.

Reporting Requirements

Requires reporting within **four business days** after the determination of materiality. The report must detail the nature, scope, and impact of the incident. There are provisions for delaying disclosure if reporting the incident could pose a substantial risk to national security or public safety.

Penalties for Non-Compliance

Penalties for non-compliance are typically industry specific. They can vary depending on the severity of the breach and the delay in reporting.

Companies that fail to disclose material incidents could face enforcement actions, including monetary penalties and other regulatory sanctions.

Additional Resources:

https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Staff Notice 51-333 – Environmental Reporting Guidance (Canada)

CSA
ACVM
Canadian Securities Administrators
Autorités canadiennes en valeurs mobilières

Canadian publicly traded companies (particularly those listed on the Toronto Stock Exchange), must adhere to cybersecurity disclosure requirements.

Regulatory Body

Canadian Securities Administrators (CSA)

Reporting Requirements

- **Immediate Disclosure via Press Release:** Once an incident is determined to be material, it must be disclosed promptly, typically through a press release. Unlike the US, there is no four business days reporting requirement.
- **Annual Reporting:** Canadian issuers must include cybersecurity risk management practices in their regular filings, detailing how these risks are identified, assessed, and managed.

Applicable Sectors

Applies to Canadian publicly traded companies across all sectors.

Penalties for Non-Compliance

Penalties for non-compliance are typically industry specific. They can vary depending on the severity of the breach and the delay in reporting.

Companies that fail to disclose material incidents could face enforcement actions, including monetary penalties and other regulatory sanctions.

Additional Resources:

https://www.osc.ca/sites/default/files/pdfs/irps/csa_20101027_51-333_environmental-reporting.pdf

Market Abuse Regulation (EU)

In the EU if a cybersecurity incident under NIS2 materially impacts a company's operations or financial performance, it could also trigger disclosure requirements under the Market Abuse Regulation (MAR). Companies listed on stock exchanges may need to disclose the incident to investors if it is deemed material.

Regulatory Body

European Securities and Markets Authority (ESMA)

What's Involved

Immediate Disclosure: Issuers of financial instruments that are listed on regulated markets are required to disclose inside information as soon as possible. "Inside information" is defined as information that could have a significant impact on the price of the company’s securities.

Delayed Disclosure: In certain circumstances, issuers can delay the public disclosure of inside information, but this is only allowed if immediate disclosure is likely to prejudice the legitimate interests of the issuer, the delay would not be likely to mislead the public and the issuer is able to ensure the confidentiality of that information.

Applicable Sectors

Applies to public companies listed on EU based stock exchanges

Penalties for Non-Compliance

- **Fines:** The penalties for non-compliance with MAR can be severe. For issuers, the maximum fines can be up to €15 million or 15% of the annual turnover, whichever is greater. For individuals, the fines can be up to €5 million.
- **Administrative Measures:** NCAs can impose a variety of administrative measures, including public censure of the issuer or individuals responsible, Orders to cease and desist from repeating the offense and withdrawal or suspension of the issuer's securities from trading on a regulated market.
- **Criminal Sanctions:** In some EU Member States, breaches of MAR, particularly those involving insider trading and market manipulation, can lead to criminal prosecution, with penalties including imprisonment.

Additional Resources:

https://www.esma.europa.eu/document/final-report-market-abuse-regulation-guidelines

About SIGA

SIGA's provides a Process-Oriented OT Cybersecurity for real-time decision-making capabilities for managing all Incident Response phases of an OT cyberattack – including Detection, Containment and Cyber Forensics. Unlike other solutions, SIGA detects all expressions of a cyber-attack based on its unfiltered view of all Levels of Cyber OT, including Level Zero visibility.

Founded in 2014, SIGA has global customers in multiple sectors including Oil & Gas, Power Utilities, Data Centers and Water.

For more information visit:
www.sigasec.com