Theodoros Ntouskas, PhD

Managing Director

The Evolving Cybersecurity Compliance Landscape

infocom SECURITY

Infocom Security Conference: 6 & 7 July 2022

ict PROTECT

INFORMATION SECURITY SERVICES

www.ictprotect.com

Our services

Law
Regulations
COMPLIANCE
Transparency
Rules
Busin
30
L
Low
6 / 38
INFRASTRUCTURE

Assurance Services

Compliance Services

Security Management Services

Training Services

STORM SaaS

Selected Clients

Alberta

ALMI TANKERS S.A.
Committed to operational integrity

DIANA SHIPPING SERVICES S.A.

inaccess

υδρόγειος
Ασφαλιστική

European Commission

SANTE
INTERNATIONAL

PAE RAE
ΡΥΘΜΙΣΤΙΚΗ ΑΡΧΗ ΕΝΕΡΓΕΙΑΣ
REGULATORY AUTHORITY FOR ENERGY

AS
NETWORK

workable

DIALECTICA
Sharing knowledge beyond borders

workadu
YOUR BUSINESS PLAYGROUND

Κοινωφελές Ίδρυμα
Ιωάννη Σ. Λάτση

ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ

ATHENS UNIVERSITY
OF ECONOMICS
AND BUSINESS

HELLENIC
AMERICAN
UNION

eltrak CAT

AMARLA

Biamax

FRONERI

uni.systems

ALGOSYSTEMS
THE PATH FORWARD

INTRASOFT
INTERNATIONAL

The Evolving Cybersecurity Compliance Landscape

- **Introduction**

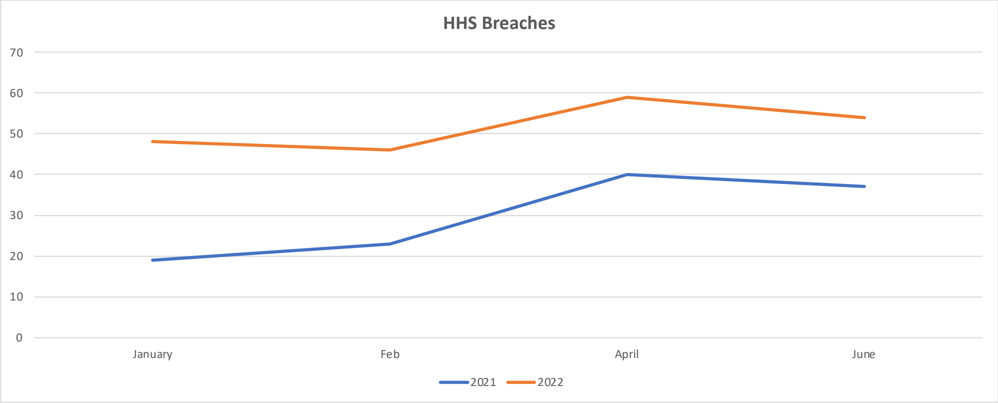
- **Current year events & changes**

- **COVID 19 "effect" in Cybersecurity**

- **Compliance Trends & Next Steps**
  - Maritime Sector
  - Energy Sector
  - Cloud Providers

Current year events & changes

The U.S. Department of Health and Human Services Office for Civil Rights Breach Portal received reports of hacking incidents nearly **double** of the incidents reported during the same period in 2021.

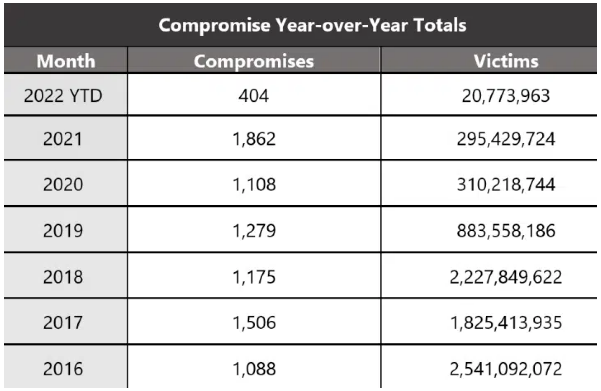


	2021	2022	% increased
January	19	48	**60%**
February	23	46	**50%**
April	40	59	32%
June	37	54	31%

Note: As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting > 500 individuals.

Current year events & changes

- According to the Q1 data breach analysis (Identity Theft Resource Center), the 404 publicly-reported data compromises in the U.S. represent a **14 % increase compared to Q1 2021**
- Approximately 92% of the data breaches in the first three months of 2022 resulted from cyberattacks. Phishing and ransomware remain the **top two root causes for data compromises.**
- Healthcare, Financial Services, Manufacturing & Utilities, and Professional Services sectors **had the most compromises in Q1 2022**.



Compromise Year-over-Year Totals		
Month	Compromises	Victims
2022 YTD	404	20,773,963
2021	1,862	295,429,724
2020	1,108	310,218,744
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935
2016	1,088	2,541,092,072

Current year events & changes

Pandemic-Related Identity Fraud Crime Victim Impacts Report.

- **4 in 10** consumers who applied for pandemic benefits since 2020 in US say their **identities were misused**
- 24 % of victims' cases **required 6 months -1 year to resolve.**
- 8 % of 2021 victims describe their cases as **unresolved in April 2022**.

Current year events & changes

ictPROTECT
INFORMATION SECURITY SERVICES

COVID-19 Pandemic Event

- New Virtual shops due to lockdown
- Remote work: the new workspace reality
- The adoption of Cloud Services has been increased
- Most of the companies adopt BYOD → no hardening → not auditable
- Internal Services → External Services: found the easy way and not the secure way → insufficient hardening
- Human errors are frequent than previous due to work from home

Top 3 trends in Cybersecurity by Gartner

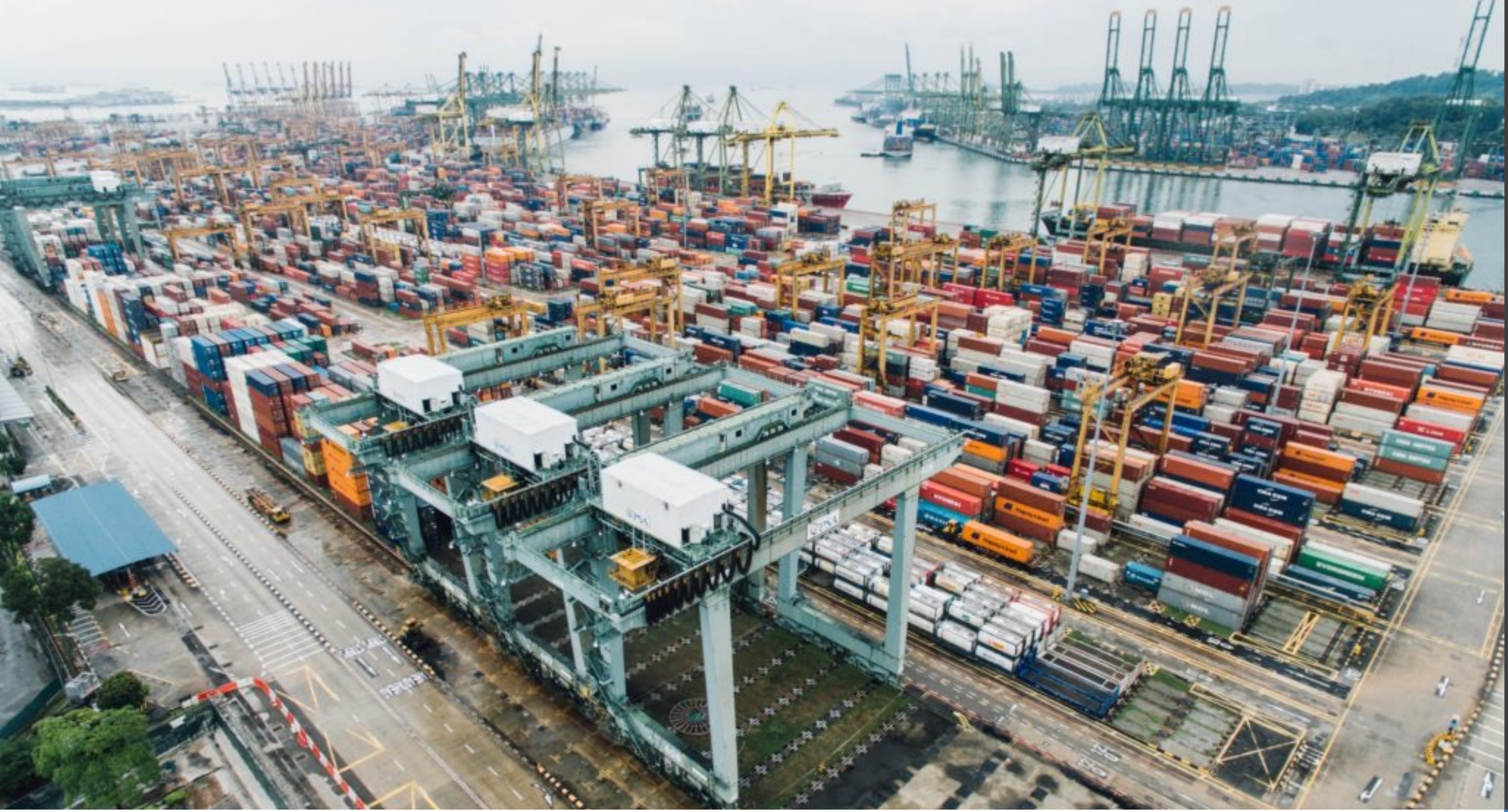
- **1. Attack surface expansion:**
  -- Remote working creates larger attack surface: 60% of knowledge workers are remote, and at least 18% will not return to the office

  --An increasingly exposed public sector: As public sector departments continue their digital transformation, more and more services vital to our daily lives are being digitised

  -- Use of cyber-physical systems have exposed new and challenging attack "surfaces."

- **2. Identity system defence**
  --Misuse of credentials is now a primary method that attackers use to access systems and achieve their goals.

- **3. Digital supply chain risk**
  --Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021



Commercial Ships & Cybersecurity Requirements

Commercial Ships & Cybersecurity Requirements

ictPROTECT INFORMATION SECURITY SERVICES

Commercial Ships

- Modern ships **cannot** be viewed as **isolated** units since:
  - **depend** on different and plethora information systems,
  - **interact** with different entities
  - any potential threats could have **significant impact** at the proper operation of all **interconnected entities**.

Top 3 trends in Cybersecurity by Gartner

- **1. Attack surface expansion:**

  -- Remote working creates larger attack surface: 60% of knowledge workers are remote, and at least 18% will not return to the office

  --An increasingly exposed public sector: As public sector departments continue their digital transformation, more and more services vital to our daily lives are being digitised

  -- Use of cyber-physical systems have exposed new and challenging attack "surfaces."

- **2. Identity system defence**

  --Misuse of credentials is now a primary method that attackers use to access systems and achieve their goals.

- **3. Digital supply chain risk**

  --Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021

Cybersecurity Requirements

- IMO 2021 - MSC.428**:** Maritime Cyber Risk Management
- **TMSA v3,** Improve and measure safety management systems
- **BIMCO v4**, Guidelines on Cyber Security Onboard Ships (2020)
- **IMO 2021 - MSC.428**: Maritime Cyber Risk Management
- Classification societies - Cyber Secure class notation

Commercial Ships & Cybersecurity Requirements

ictPROTECT
INFORMATION SECURITY SERVICES

IMO
IMO's
MSC-
FAl.1-
Circ.3

Classificaiton Soc.

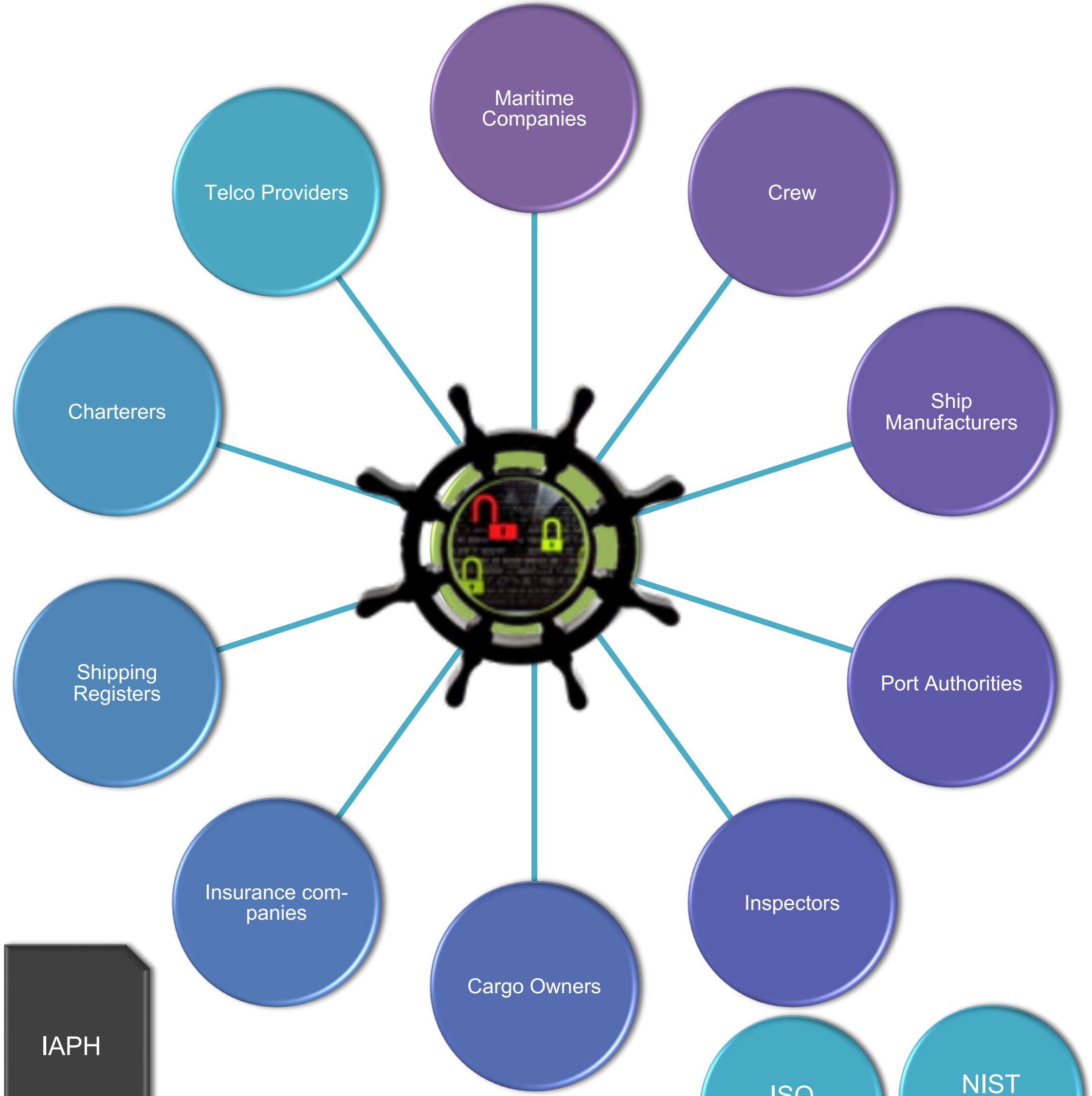
Cyber secure class notation

TMSA3

BIMCO

Us Coast Guard, Feb. 2020

IACS, rec.166



Maritime Companies

Telco Providers

Crew

Charterers

Ship Manufacturers

Shipping Registers

Port Authorities

Insurance com-panies

Cargo Owners

Inspectors

ISO 27001

ISO 22301

ISO 27701

SOC 2

GDPR

CCPA

ISO 27002

NIST CSF

ENISA

UK DfT

IAPH

Energy Sector – Cybersecurity Requirements

Energy Sector – Cybersecurity Requirements

ictPROTECT INFORMATION SECURITY SERVICES

Power Plants

- Need for **Energy Autonomy**
- Large Plants are deployed (1 GW – 2GW)
- Modern Power Plants (Solar, Wind, Battery Storages):
  - are **managed remotely**
  - sites from different locations are **connected / managed as one site**
- number of cyberattacks in the energy field has been **continuously increased**
- any potential threat could have **significant impact** at the proper operation of all **interconnected entities**.

Top 3 trends in Cybersecurity by Gartner

- **1. Attack surface expansion:**

  -- Remote working creates larger attack surface: 60% of knowledge workers are remote, and at least 18% will not return to the office

  --An increasingly exposed public sector: As public sector departments continue their digital transformation, more and more services vital to our daily lives are being digitised

  -- Use of cyber-physical systems have exposed new and challenging attack "surfaces."

- **2. Identity system defence**

  --Misuse of credentials is now a primary method that attackers use to access systems and achieve their goals.

- **3. Digital supply chain risk**

  --Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021

Cybersecurity Requirements

- NIS 1 / NIS 2
- UK: Energy Networks Association (ENA)-EREC G99
- UK: NCSC Cyber Assessment Framework (CAF)
- North American Electric Reliability Corporation (NERC) CIP

Energy Sector – UK Requirements

- Engineering Recommendation G99, (EREC G99), was issued by the **Energy Networks Association** (ENA). Generators are now classified into different types:
  - Type A: 0.8kW to < 1MW and connecting at a voltage <110kV,
  - Type B: 1MW to <10MW and connecting at a voltage <110kV,
  - Type C: 10MW to <50MW and connecting at a voltage <110kV,
  - Type D: ≥ 50MW or connecting at a voltage ≥ 110kV)

  - Distributed Energy Resources (DER) - Cyber Security Connection Guidance (CSCG) based on the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF):
    - Promote cyber security throughout the **design, development, deployment, connection and maintenance of new DER projects**.
    - Provide a **consistent approach** to cyber security for DER connections.
    - Provide a **baseline level** of cyber security for new DER connections
    - Assist the Department for Business Energy and Industrial Strategy (BEIS), NCSC and the Energy Networks Association (ENA) **to identify short-term and long-term threats** and promote standardisation
    - Provide cyber security guidelines that are flexible, regardless of size, maturity or location
    - Influence technology providers to **improve security** for their devices out of the box
  - Energy Delivery Systems – Cyber Security Procurement Guidance:
    - **Defining** and **mapping** of **asset** and technology areas for Energy Delivery Systems (EDS)
    - Developing of a **cyber security reference model** for the asset and technology areas or zones
    - **Reviewing existing procurement language** references, good practice and international standards for cyber security that may be relevant to EDS
    - Determining **cyber security requirements** to deliver target cyber security levels which can be aligned to the reference model
    - **Developing cyber security procurement guidance statements** (CSPG) that will enable procured products and services to meet the cyber security requirements identified

- NCSC Cyber Assessment Framework (CAF). aims at **improving government cyber security.** It is applicable also for:
  - organisations **within the UK Critical National Infrastructure (CNI)**
  - organisations subject to Network and Information Systems (NIS) Regulations
  - organisations **managing cyber-related risks to public safety**

North American Electric Reliability Corporation (NERC) CIP

North American Electric Reliability Corporation (NERC) defines the reliability requirements for planning and operating the North American bulk power systems

- NERC develops and enforces reliability standards known as NERC Critical Infrastructure Protection (CIP) standards
- All bulk power system owners, operators, and users must comply with NERC

CIP standards apply to the BES:

- **100kV** and above, but with some exceptions, primarily for radial lines
- **20MVA** and above generating units, 75MVA and above generating plants, with some exceptions for wholly behind-the-meter generation
- Includes Control Centers that monitor and control the BES

** **Bulk Electric System (BES):** All Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher.

NERC CIP – Key requirements

Delivery Phase

- Asset Inventory (Review and update changes)
- Asset Classification
- Cyber security policies should be in place
- Cyber security plans should be in place (Awareness, Physical Security Controls, Electronic Access Controls, Incident Response plan etc.)
- Documented Cyber Security roles and responsibilities
- Training on Cyber security threats, incident management, recovery plans etc.
- Documented personnel Risk Assessment
- Criminal History Record (Perform and evaluate checks for authorized access)
- Network controls (firewalls, access rights, VLANs, authentication, strong passwords, encryption, IDS)
- Monitoring systems
- Identification and protection of information (Classification, storage, transit, use)

Security Operator

- Incident Handling procedures (detection of malicious code, event logging)
- Incident Reporting and Response (Identify, classify, respond, testing incident response plan, retain records, document lessons learned, update plan, notify)
- Recovery Plans (backup, storage, preserve data, testing, document lessons learned, update plan)
- Configuration (OS, Software installed, logical network accessible ports, security patches)
- Conduct a vulnerability assessment
- Document and implement Supply Chain Cyber Security Risk Management plan(s)
- Risk Assessment (Transmission stations, substations, primary control centers)
- Physical Security Plan (Transmission stations, substations, primary control centers)

Network Operator

- Documented Cyber Security roles and responsibilities
- Purdue Model implementation defining the different levels of critical infrastructure that are used in production lines and the way to secure them.
- Physical and Electronic Access Controls (Authorization records, electronic access, privileges, security perimeter, cabling, visitor logs)
- Offboarding (termination of accounts, change passwords for shared accounts)
- Monitoring physical security perimeter (alarms, alerts, access logs retention)
- Network and System monitoring
- Change Management (Document changes of configuration, verify, test changes, monitor)
- Patch management process (tracking, evaluating, installing cyber security patches for applicable Cyber Assets)
- Mitigation Plan (mitigate vulnerabilities of security patches)
- Deter, detect, prevent malicious code (mitigate threats, use of signatures or patterns)

Energy Sector – Cybersecurity Requirements

Power Plants

- Need for **Energy Autonomy**
- Large Plants are deployed (1 GW – 2GW)
- Modern Power Plants (Solar, Wind, Battery Storages):
  - are **managed remotely**
  - sites from different locations are **connected / managed as one site**
- number of cyberattacks in the energy field has been **continuously increased**
- any potential threat could have **significant impact** at the proper operation of all **interconnected entities**.

Cybersecurity Requirements

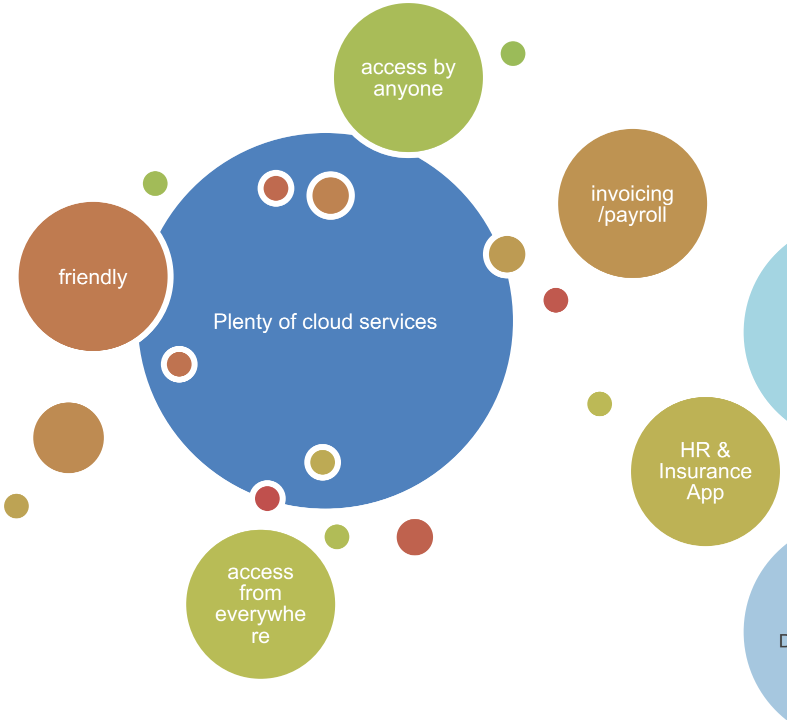
- NIS 1 / NIS 2
- UK: Energy Networks Association (ENA)-EREC G99
- UK: NCSC Cyber Assessment Framework (CAF)
- North American Electric Reliability Corporation (NERC) CIP

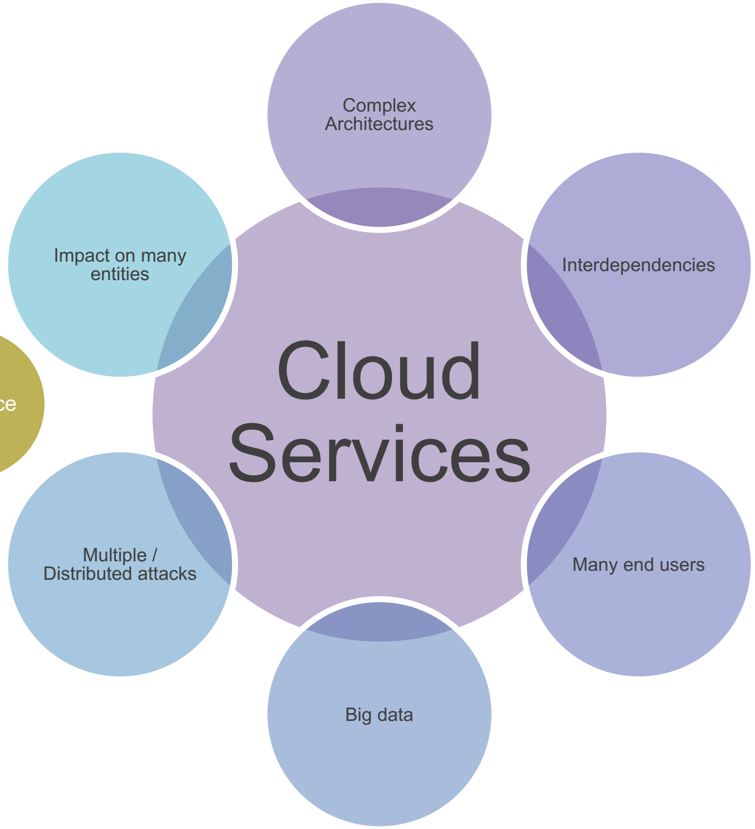
Guidelines & Standards

- **ISO/IEC 27001:2013** - Information technology - Security techniques - Information security management systems - Requirements.
- **ISO/IEC 27017: 2015** - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27019: 2017** - Information technology - Security techniques - Information security controls for the energy utility industry.
- **Cloud Security Alliance (CSA) STAR program** - Defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud.
- **AICPA SOC 2 Type 2 attestation** - A restricted use report intended to report on controls relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy system attributes.
- **US Government FedRAMP authorization** - The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by federal agencies.
- **NIST SP 800-53 Rev. 5** - Security and Privacy Controls for Information Systems and Organizations.
- **ISA/IEC 62443**: requirements related to cyber security for products intended for use in the **Industrial Automation and Control Systems (IACS)** environment
- National Renewable Energy Laboratory (NREL) The certification testing procedure can potentially be used in a U.S. industry standard to address diverse manufacturer approaches to cybersecurity and to inform the development of appropriate third-party conformity assessment programs for DER cybersecurity testing and certification.
- NISTIR 7628: Guidelines for Smart Grid Cybersecurity
- ENISA: Communication network dependencies for ICS/SCADA Systems
- **SANS 800-82**: Guide to Industrial Control Systems (ICS) Security

Third Party Risk / Resiliency & Cloud Security Requirements

Third Party Risk / Resiliency & Cloud Security Requirements





Third Party Risk / Resiliency & Cloud Security Requirements

ictPROTECT
INFORMATION SECURITY SERVICES

"Must Have" features of cloud services

- Providing True Multi-tenancy
- Regularly Delivered, Vendor-Managed Updates
- World-Class Data Center and Security
- A High-performance Sustainable Infrastructure
- Faster Deployment (Infrastructure as Code)
- Control of Client Data

Cybersecurity Requirements

- Shared roles and responsibilities within a cloud computing environment
- Removal of cloud service customer assets
- Segregation in virtual computing environments
- Virtual machine hardening
- Administrator's operational security
- Monitoring of cloud services
- Alignment of security management for virtual and physical networks

Top 3 trends in Cybersecurity by Gartner

- **1. Attack surface expansion:**

  -- Remote working creates larger attack surface: 60% of knowledge workers are remote, and at least 18% will not return to the office

  --An increasingly exposed public sector: As public sector departments continue their digital transformation, more and more services vital to our daily lives are being digitised

  -- Use of **cyber-physical systems** have exposed new and challenging attack "surfaces."

- **2. Identity system defence**

  --Misuse of **credentials** is now a primary method that attackers use to access systems and achieve their goals.

- **3. Digital supply chain risk**

  --Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021

Guidelines & Standards

- **ISO/IEC 27001:2013** - Information technology - Security techniques - Information security management systems - Requirements.
- **ISO/IEC 27017: 2015** - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- **ISO/IEC 27018:2019-** Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO/IEC 27019: 2017** - Information technology - Security techniques - Information security controls for the energy utility industry.
- **Cloud Security Alliance (CSA) STAR program** - Defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when transitioning their IT operations to the cloud.
- **AICPA SOC 2 Type 2 attestation** - A restricted use report intended to report on controls relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy system attributes.

Mapping of Standards

Mapping of Standards

Standard	Purpose	Information	Controls	Target	Certification
HIPAA	Standard for **sensitive patient data protection**.	Protection of Protected Health Information and Electronic Protected Health Information.	Privacy, Security and Breach Notification Rules for PHI and ePHI	Covered Entities and Business Associates	No certification is endorsed
ISO 27017	Standard for **cloud service customers** and **cloud service providers**	Protection of Information stored in the cloud	Based on ISO/IEC 27001, 27002 security controls. Provides additional controls to address cloud-specific information security threats and risks considerations.	Cloud Service Providers and Cloud Service Customers	ISO certification is endorsed
ISO 27018	Standard for privacy of Personally Identifiable Information **(PII) stored in the cloud**	Protection of Personally Identifiable Information (PII) stored in the cloud	Based on ISO/IEC 27001, 27002 security controls. Emphasizes in additional controls to increase the level of protection of personal data in cloud services.	Cloud Service Providers act as PII Controller, PII Processor	ISO certification is endorsed
ISO 27701	Standard for an effective **Privacy Information Management System**	Protection of Personally Identifiable Information (PII)	Based on ISO/IEC 27001, 27002 security controls. Provides additional controls for PII Controllers and PII Processors	PII Controller, PII Processor	ISO certification is endorsed (ISO 27001 is prerequisite)
SOC 2 (AICPA TSC)	Standard to help Organizations protect customer information and **data stored in cloud-based infrastructures**.	Protection of Customers data	SOC 2: focus on Information and IT Security related to Security, Availability, Processing, Integrity, Confidentiality and Privacy. SOC 3: same with SOC 2 but for public distribution	Organizations that process customers data in cloud services	SOC 2 Report is endorsed
ISA/IEC 62443 4-1	Defines **SDL** requirements related to cyber security for products intended for use in the **Industrial Automation and Control Systems (IACS)** environment	Protection of IACS	Security requirements definition, Secure design, Secure implementation (including coding guidelines), verification and validation Patch management and product end-of-life.	IEC 62443-4-1 applies to the developer and maintainer of the product and are not applicable to the integrator or the user of the product	ISA/IEC 62443 4-1 Certification is endorsed

Our Proposed Compliance Methodology

Phase I: Define Information Security Team

- Appoint CISO
- Assign security responsibilities to key personnel (i.e. Security Engineers, DevOps, Department Managers)

Phase II: Cartography

- Identify Information Assets. This may include assets related to PII, PHI, etc. (Data, Software, Hardware)
- Identify their dependencies
- Identify the core business requirements
- Identify key suppliers

Phase III: Conduct Readiness Assessment

- Map ISO 27001 & NIST controls with AICPA TSC requirements, ISO 27017, ISO 27018, ISO 27019, ISO 27701, etc.
- Identify existing controls and find grey areas

Phase IV: Evaluate Key suppliers

- Evaluate their technical controls (TFA, Encryption, Backup, remote access etc.)
- Evaluate Support Services & SLAs & DPA
- Compliance with applicable regulation (i.e. GDPR, CCPA, NERC CIP, etc.)

Phase V: Technical Security Assessment

- Product security context
- Threat model
- Product security requirements
- Product security requirements content
- Security requirements review

Phase VI: Conduct Risk Assessment & Risk Treatment Plan

- Conduct Impact Assessment
- Identify Potential Threats
- Evaluate Vulnerabilities
- Propose Mitigation Actions

Phase VII: Develop technical & organizational controls

- Security Policies & Procedures
- SLAs with key suppliers
- DPA with data processors
- Hardening and automation as possible

Phase VIII: Develop Contingency Plan

- Identify recovery priorities
- Identify dependencies
- Establish communication lines (internally and with the key suppliers)
- Create Runbooks in case of unwanted event

Phase IX: Conduct Training & Awareness Programs

- Security Policies & Procedures
- Remote work and Business continuity scenarios

Phase X: Monitor, audit, and update security measures on an ongoing basis

- Internal Audits
- Review of Technical & Organization controls

Let's do business

info@ictprotect.com

ictPROTECT
INFORMATION SECURITY SERVICES