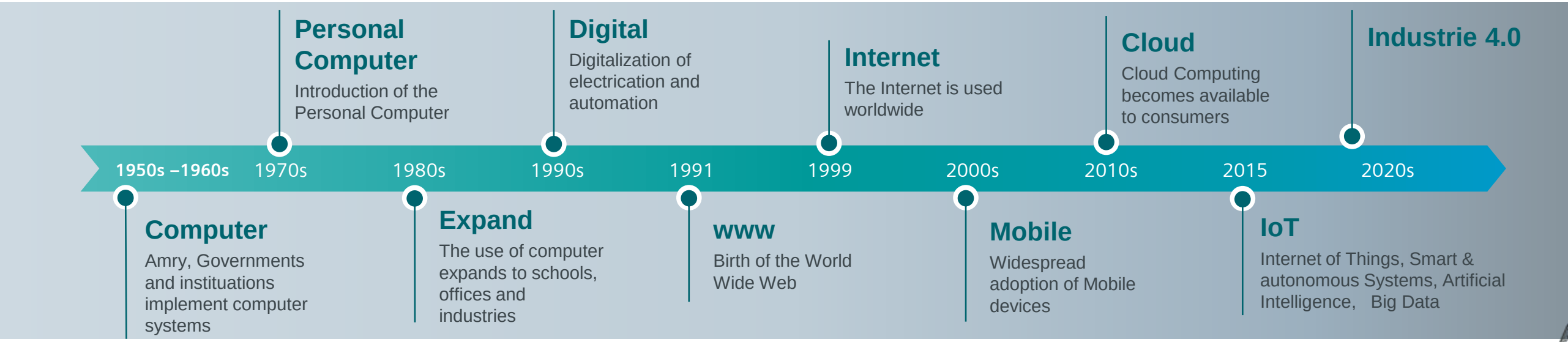
SIEMENS
Ingenuity for life

How does the implementation of the recent EU NIS directive impact power plant operation?

Frédéric Buchi I Cyber Security Consultant

Cyber attacks are increasingly focusing on critical infrastructure

SIEMENS
Ingenuity for life

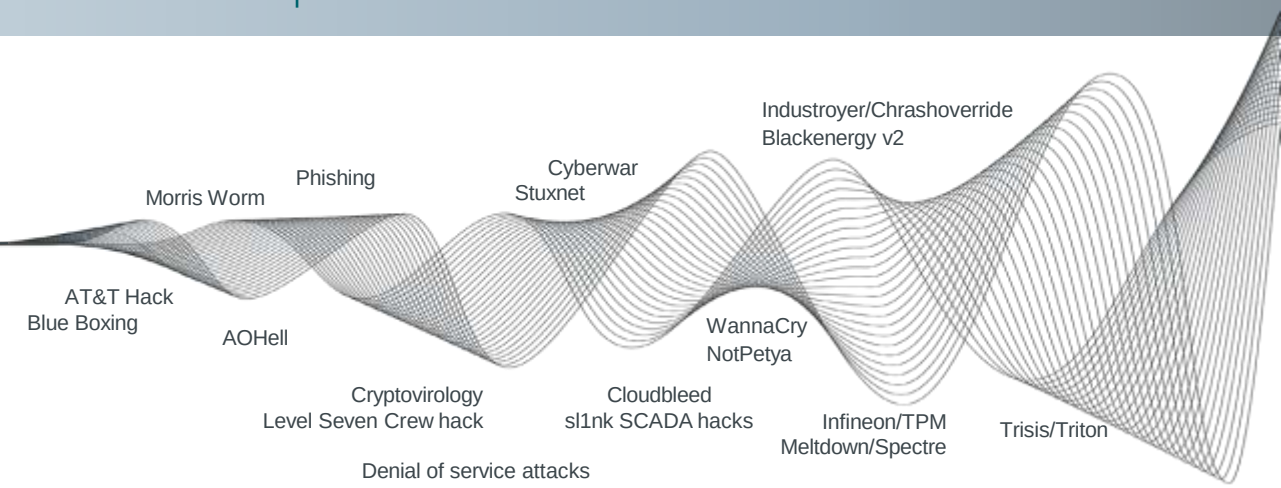


The **Treat Landscape increases** and **changes** countinuously –

Attacks increasingly focus on industrial Systems and **Critical Infrastructures**

600 **Billions EUR**

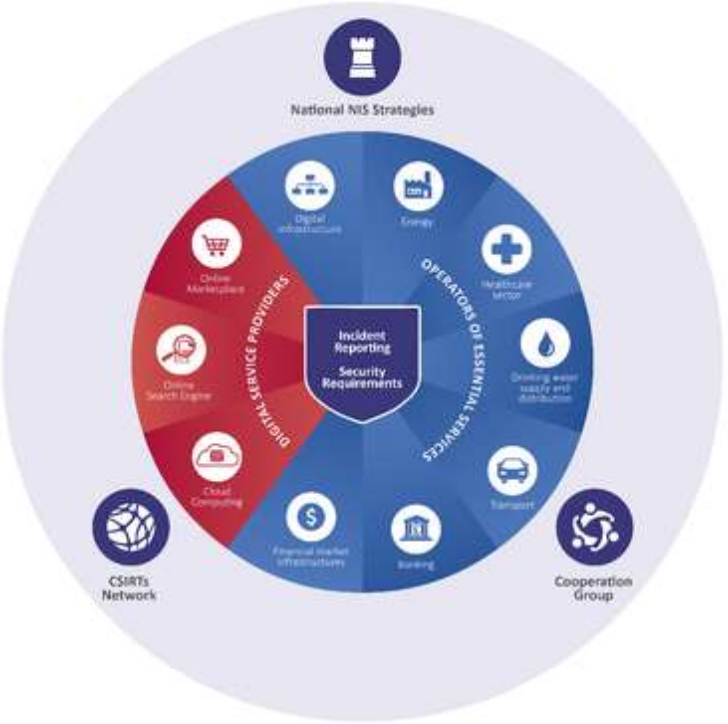
Damages in 2018 due to Cyber Attacks



What is the EU directive 2016/1148, also known as the NIS Directive?

SIEMENS
Ingenuity for life

- An instrument introduced by th European Commission to ensure that every EU Member States introduces a cyber security legislation applying to so-called Operators of Essential Services (OES) and Digital Service Providers (DSP)
- Additional important objective is to ensure that incidents are reported and coordinated by national CERTs
- Provides some flexibility to EU Member States to define themselves the specific obligations applying to the OES and DSP (unlike GDPR)
- Deadlines:
  - Transposition into national law by May 9th, 2018
  - Identification of the Operators of Essential Services by Nov. 2018



Source: ENISA

CERT: Computer Emergency Response Team
NIS: Network and Information Security
GDPR: General Data Protection Regulation

Transposition of the EU NIS Directive
Example: NIS Law in Austria

SIEMENS
Ingenuity for life

Implementation of Cyber Security Measures

- Risk based
- State of the Art
- Proportionate & appropriate
- Based on International Standards and ENISA recommendations

- ISO/IEC 27001
- Sector-specific Standards:

  for Energy: BDEW-Whitebook

Proof of certification or audits

- 1 year after identification as OES
- Subsequently every 3 years
- Verification by local authorities – Austrian BMI

Identification of a Contact Person

Mandatory reporting of significant incidents

Volontary reporting of incidents
Information exchange

Austrian Energy CERT

The ISO 27000 family of standards is establishing itself as the international standard of choice for NIS laws

BDEW: Bundesverband der Energie- und Wasserwirtschaft
BMI: Bundesminister für Inneres / Ministry of Interior
CERT: Computer Emergency Response Team
ENISA: European Union Agency for Network and Information Security
OES: Operator of Essential Services

What is enclosed in ISO/IEC 27001

SIEMENS
Ingenuity for life

ISO 27001 – Information security management systems – Requirements

Annex A - 114 security controls grouped in 14 sections

ISO 27002 – Code of practice for information security controls

Guidance for the implementation of ISO 27001 Annex A

ISO 27019 – Security control for the energy utility industry

Adaptation of ISO 27002 for its use in the Oil and Energy sectors

Power Plants are already operating (mostly) - They already have a process landscape

SIEMENS
Ingenuity for life

A typical starting point:

- ✓ Your management has defined a mission statement
- ✓ Risks to safety, environment, plant availability are evaluated before performing changes
- ✓ You ensure that your staff is trained and reach to your suppliers for additional expertise
- ✓ You monitor the efficiency of your operations and improve them continuously
- ✓ You react on incidents and ensure that lessons are learned out of them

Do you operating processes cover Cyber Security aspects

Are those processes documented?

Impact of NIS legislation in operation
Example #1 – Operations Security & Change Management

SIEMENS
Ingenuity for life

ISO 27001 requirement

A.12 Operations security		
A.12.1 Operational procedures and responsibilities		
Objective: To ensure correct and secure operations of information processing facilities.		
		Control
A.12.1.2	Change management	Ch ce be

ISO 27002 implementation guidance

12.1.2 Change management

Control

Changes to the organization, business processes, information proc ilit
should be controlled.

Implementation guidance

In particular, the following items should be considered:
a) identification and recording of significant changes;
b) planning and testing of changes;
c) assessment of the potential impacts, including information secu acts, c
d) formal approval procedure for proposed changes;
e) verification that information security requirements have been me
f) communication of change details to all relevant persons;
g) fall-back procedures, including procedures and responsibilities f orting ar
unforeseen events;
h) provision of an emergency change process to enable quick and olled im
incident (see 16.1).

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes. When changes are made, an audit log containing all relevant information should be retained.ca

Example of implementation:

- ✓ Extend the current change management process as to include an assessment of cyber risk
- ✓ Include the Cyber Security Officer in the review
- ✓ Document the secure configuration of the system for emergency fallback and restoration

Impact of NIS legislation in operation
Example #2 – Incident Handling

SIEMENS
Ingenuity for life

NIS directive requirement

3. Member States shall ensure that operators of essential services notify, without und delay, th authority or the CSIRT of incidents having a significant impact on the continuity of the ntial se provide. Notifications shall include information enabling the competent authority or the RT to d cross-border impact of the incident. Notification shall not make the notifying party subje increa

ISO 27001 implementation guidance

A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements		
Objective: To ensure a consistent and effective approach to the management of in n se incidents, including communication on security events and weaknesses.		
A.16.1.1	Responsibilities and procedures	*Control* Management responsibilities and procedures s tab to ensure a quick, effective and orderly respon rm security incidents.
A.16.1.5	Response to informa-tion security incidents	*Control* Information security incidents shall be respon n acc with the documented procedures.

ISO 27019 implementation guidance

16.1.5 Response to information security incidents
Additional implementation guidance for ISO/IEC 27002:2013, 1
Response activities should include communications towards oth ntities w or that can draw consequences from the incident itself or from t ecided r specific CSIRT is established to that purpose it should be informed as required.
Collecting evidence can be in conflict with the need of timely system restoration to meet high availability requirements and ensure secure energy supply. The energy utility organization should define in which cases and for which systems evidence collection is possible (see 16.1.7).

Example of implementation:

- ✓ Identify reporting requirements (internal reporting, authorities, national CERT)
- ✓ Identify reporting criterias and responsibilities
- ✓ Prepare an Incident Response Plan
- ✓ Secure support from suppliers
- ✓ Train the involved staff

To address customer needs Siemens offers cyber security packages tailored to regulatory requirements

SIEMENS
Ingenuity for life

Assess and Plan

Assessments

- Cyber Gap Assessment
- Vulnerability Assessment
- Baseline Compliance Assessment

Security Processes

- Incident Response Plan preparation & testing
- Disaster Recovery Plan preparation & testing

Protect

DCS Security Controls

- Secure Architecture
- Security Documentation
- Device Hardening
- Malware Pattern Updates
- Application Whitelisting

Additional Controls

- Data Diode
- OT Security Training

Detect and Respond

Asset Management

- Asset Inventory and Change Monitoring

Multi-vendor

Powered by PAS

Vulnerability & Patch Management

- SPPA-T3000 Patch Management
- Advanced Vulnerability Management

Multi-vendor

Powered by tenable network security

Monitoring

- SPPA-T3000 Security Event Monitoring
- SPPA-T3000 Change Monitoring

Detection & Response

- SPPA-T3000 Network Intrusion Detection System
- Incident Response Retainer
- Network Anomaly Detection

Multi-vendor

Powered by DARKTRACE

Contact

Frédéric Buchi

Cyber Security Consultant Region Europe
Siemens AG
Gas and Power

siemens.at/future-of-energy