NMBU

Norwegian University
of Life Sciences
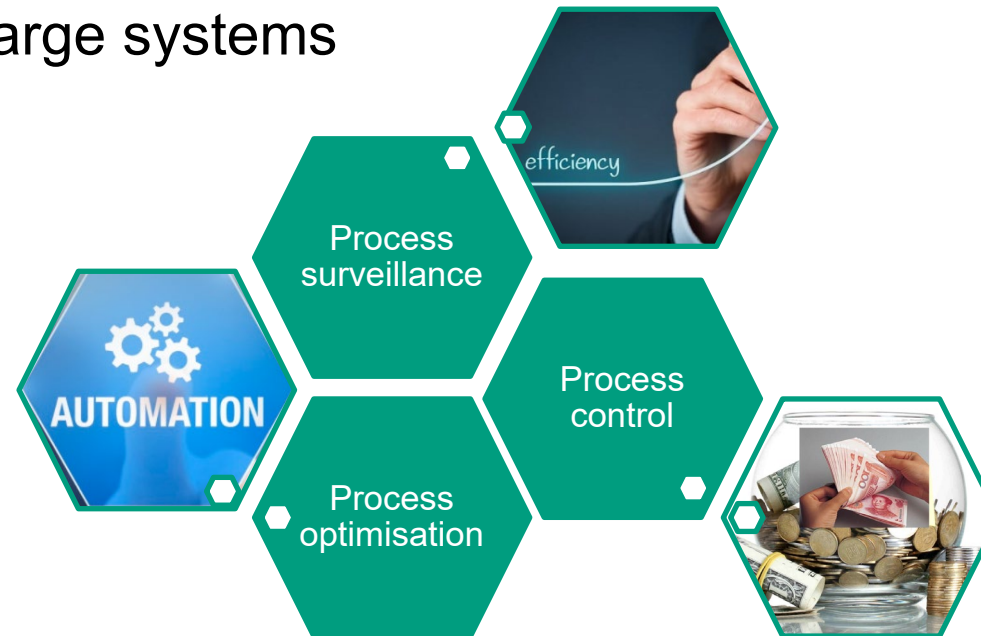
Cyber Security in the Water Sector

Outline

- Introduction

- Cyber security challenges in the water sector

- Cyber security laws

- Summary

Recent developments in digitalisation has changed to world – also the water sector

- **Advantages are numerous**: automation, adaptability, efficiency, functionality, reliability, safety, and usability of large systems

- **But there is a catch**: exposure to an expanded attack surface…

Threats

The transition to digital water provides invaluable opportunities for **enhancing operational efficiency** and **resiliency** in the water sector. However, it results in increased risks posed by adversaries and threat actors

- **System failures** (e.g., a hardware failure, software bug, a flaw in a procedure, etc)

- **Natural phenomena** (e.g., a storm, lightning, flood, earthquake, wildfire, etc)

- **Human errors** (e.g., a mistake, or lack of awareness, etc)

- **Third party failures**(e.g., a power cut, or an internet outage, etc)

- **Malicious actions** – **cyber attacks**

Types of cyber attacks

- **Denial of service:** flooding a resource (a network or web server) with thousands of false requests so as to crash or make the resource unavailable to its intended users

- **Man-in-the-middle**: an attacker embeds itself within a communication between two devices to either eavesdrop/manipulate messages or impersonate one of the devices, making it appear to be a normal exchange of information

- **Worm:** malicious program that replicates itself and spreads to other computers

- **Phishing:** fake websites or e-mail messages that look genuine and ask users for confidential personal data or to deploy malicious software on the victim's computer like **ransomware**

Vulnerabilities

- **Types of vulnerabilities**

o cyber, cyber-physical, and physical vulnerabilities

- **Causes of vulnerabilities**

o Isolation assumption

o Increased connectivity

o Easier escalation from a single unit failure to system collapse

o Cascading effects between critical infrastructure (e.g. water and energy)

# Vulnerabilities

- **Communication vulnerabilities**

  o Vulnerable protocols

  o Direct access to remote field devices such as RTUs and PLCs

- **Software vulnerabilities**

  o Vulnerabilities in Internet exposed devices that are connected to the local network (e.g. servers in the control center, employees' portable devices)

- **Physical exposure** of many ICS components, such as RTUs and PLCs - insufficient physical security

Possible attack points to modern SCADA systems
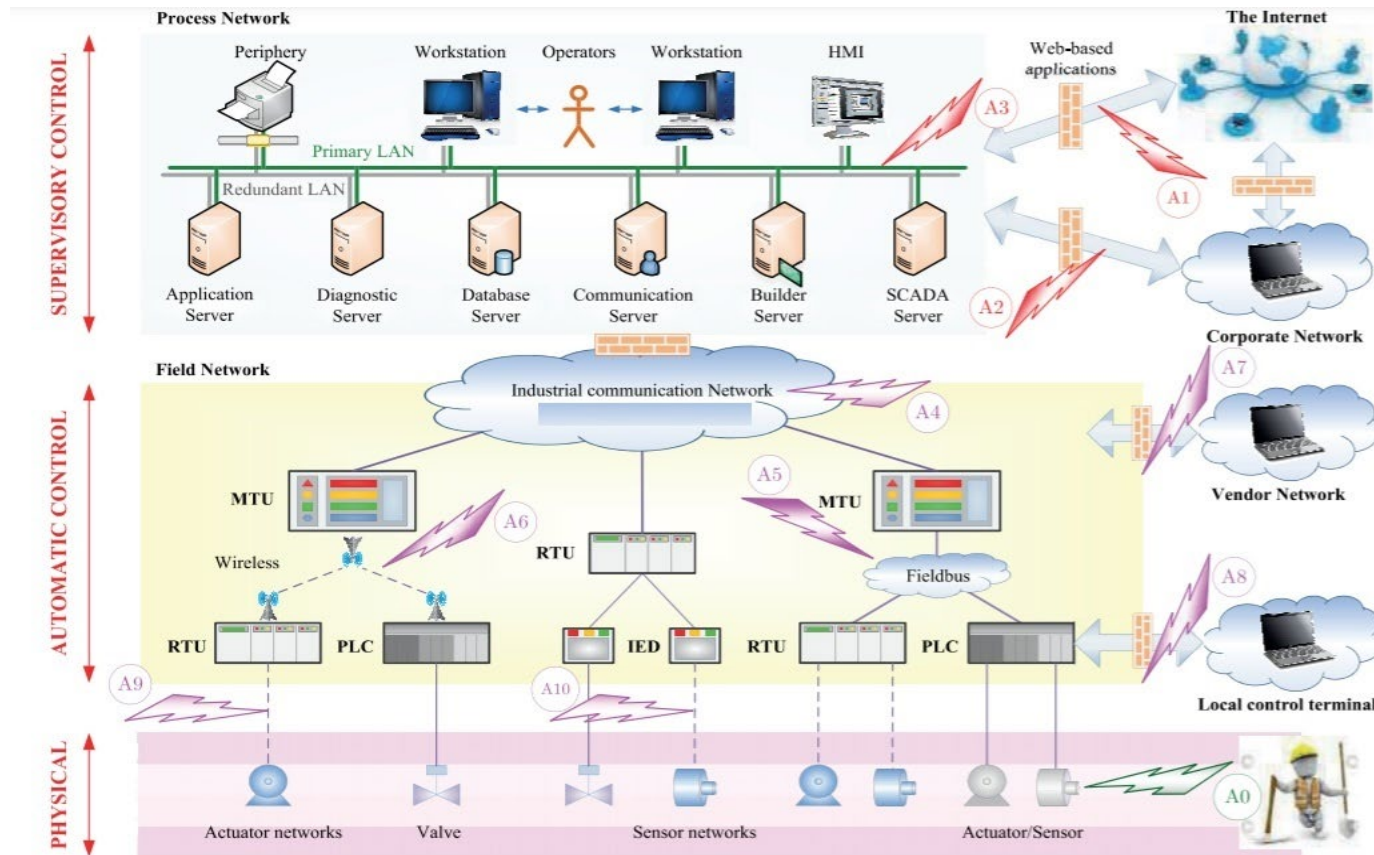
The attackers are also interetsed in the water sector

- Already a prominent target (**3rd most targeted**).

- Many cybersecurity incidents go either **undeteded and unreported**, or undisclosed. (reputation+ customers trust)

- **Cyber security** is of course already part of the agenda for water companies.

- **Physical security** has been part of the agenda for some time.
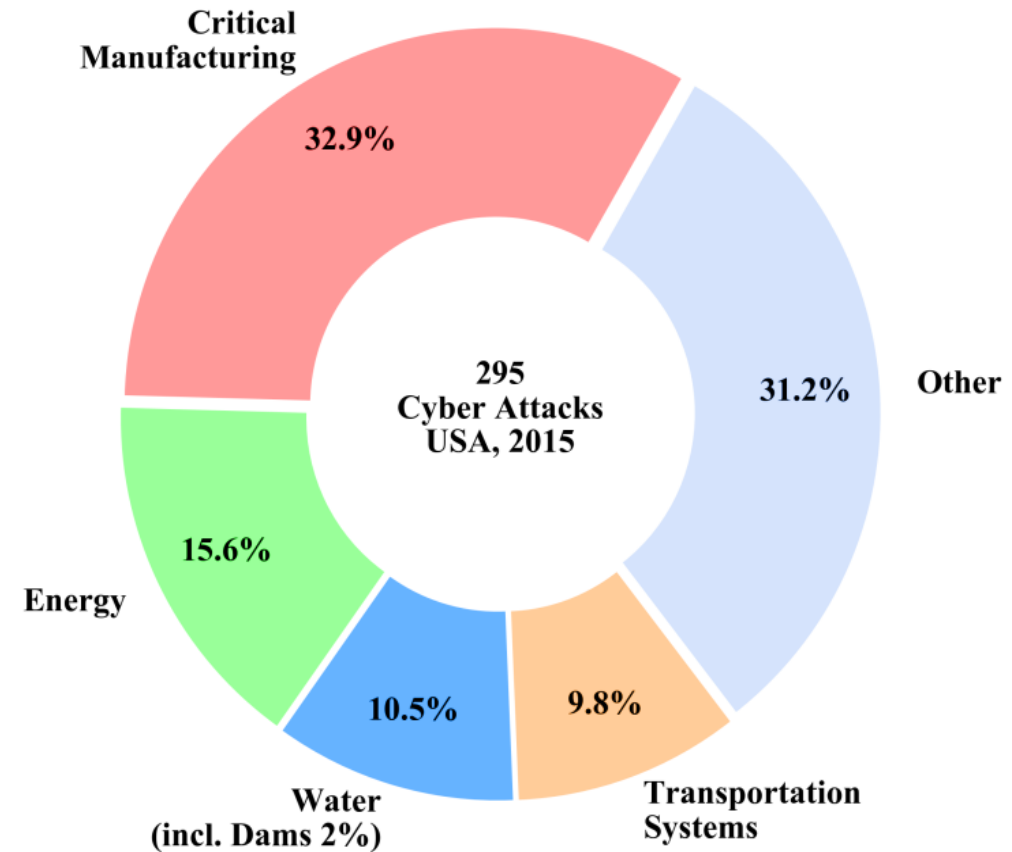
What can cyber attacks do?

- Interfere with operations – over/under dosage

- Unauthorised changes to programmed instructions; reduced pressure, overflow of sewage, malfunction of unit processes

- Modify control systems to produce unpredictable results

- Block data or send false information to operators

- Change alarm thresholds or disable them

- Prevent access to account information

- Access to personal information (GDPR directive)

- Ransomware

WaterISAC
Security Information Center

10 Basic Cybersecurity Measures:
Best Practices to Reduce Exploitable
Weaknesses and Attacks

October 2016

Cyber attack incidents

| Incidents	Year	Target	Attribution	Infection Vector	Details	Impact
Israel's water system	2020	OT	Hacktivist/ Nation state	Unknown	Israeli government reported cyber-attacks against water supply and treatment facilities and urged these facilities to change passwords.	Unknown.
Northern Colorado	2019	OT	Cybercrime	Ransomware	Locked access to technical and engineering data.	Disruption, took about three weeks to unlock data.
Kemuri water	2016	OT	Hacktivist	Remote access	Accessed PLC responsible for controlling water treatment chemicals.	Engineers were able to identify and reverse the changes made to process control parameters.
Bowman Avenue Dam	2016	OT	Hackers/ Nation state	Remote access	According to US authorities, hackers linked to Iranian Armed Forces infiltrated ICS of Bowman Avenue Dam and accessed the SCADA for the dam.	Data exfiltration and over $30k on remediation costs. Physical damage was not possible due to disconnected sluice gates.
Florida Wastewater	2012	IT	Ex-Employee	Remote access	Stolen login credentials were used to access district's computer system.	Deleting and modifying information. Ex-employee was arrested on account of computer crime.

Cyber attack incidents

edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html

CNN US   Crime + Justice   Energy + Environment   Extreme Weather   Space + Science   Edition ˅

Florida water treatment facility hack used a dormant remote access software, sheriff says

By Alex Marquardt, Eric Levenson and Amir Tal, CNN

Updated 2203 GMT (0603 HKT) February 10, 2021
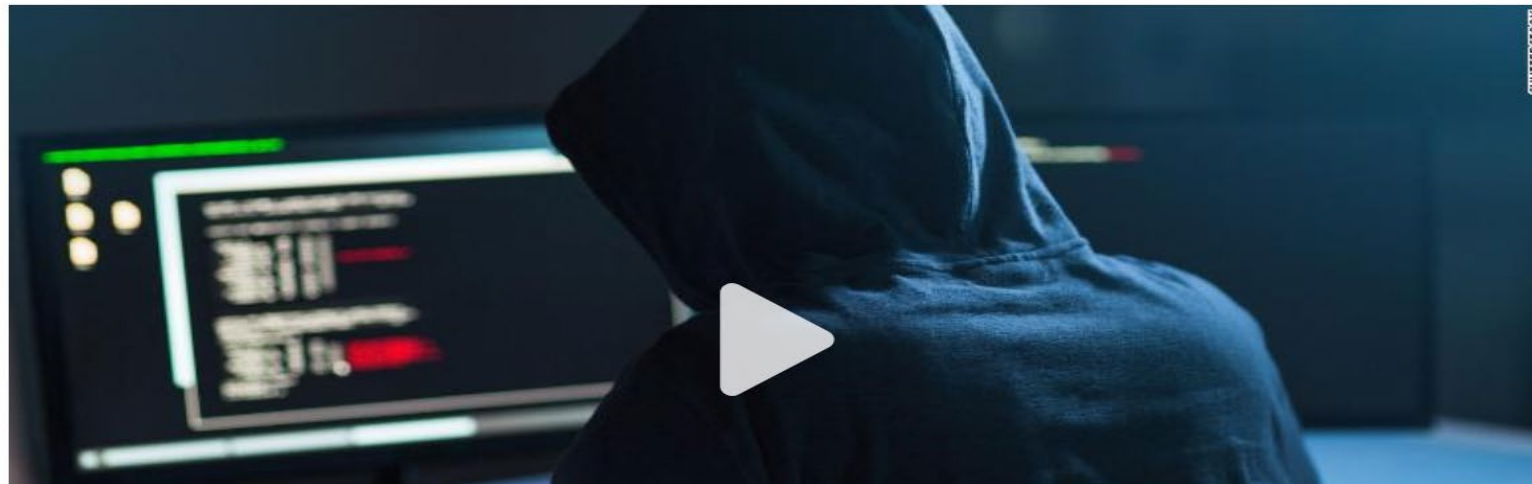
Florida water treatment cyber attack incident
Summary of the incident

- In February, 2021, attackers accessed the control system's software at the **Oldsmar water-treatment facility in Florida**, and attempted to increase the levels of **sodium hydroxide (lye)** that is used in water treatment to regulate acidity levels by adjusting the control setting to **more than 100 times** its normal levels (100ppm to 11,100ppm)

- The change was immediately detected by a plant operator, who changed the setpoint levels back before the attack had any impact on the system

- The attack used **stolen credentials** that were shared beetween multiple users and devices to remotely login to the HMI station controlling the water systems
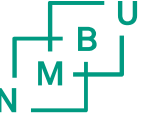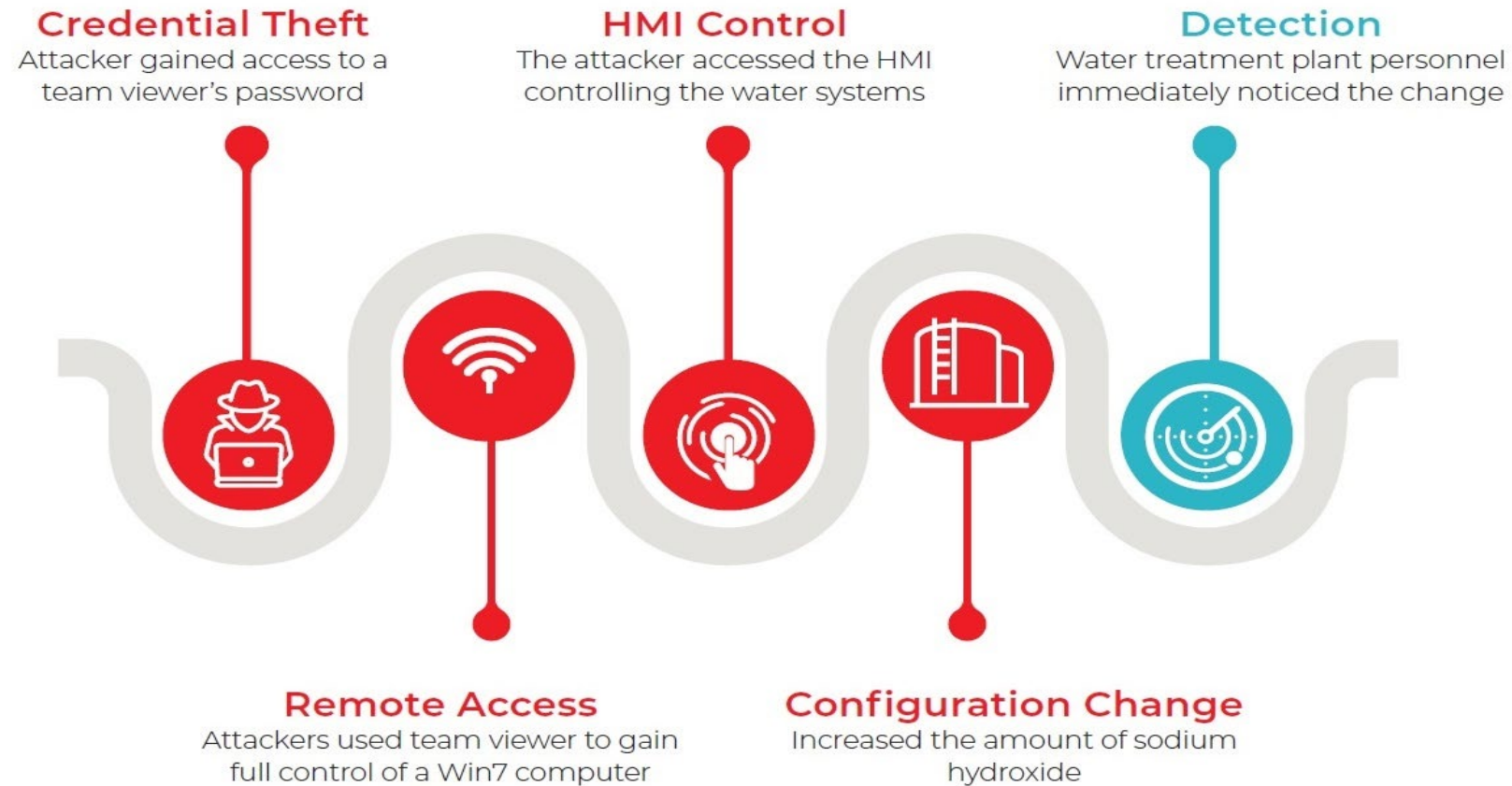
Florida water treatment cyber attack incident
Attack highlights

- The attackers accessed the Oldsmar water-treatment facility's control system via **TeamViewer**, which is a remote access software

- All computers used by the facility personnel were connected to the OT control system that used an **outdated operating system (Windows 7)**

- All computers shared the same password for remote access, and appeared to be connected directly to the Internet without any type of firewall protection

Florida water treatment cyber attack incident
Attack timeline

Credential Theft
Attacker gained access to a team viewer's password

HMI Control
The attacker accessed the HMI controlling the water systems

Detection
Water treatment plant personnel immediately noticed the change

Remote Access
Attackers used team viewer to gain full control of a Win7 computer

Configuration Change
Increased the amount of sodium hydroxide

What are the potential impacts of the incident?

- This specific incident did not result in any public health impacts, however the attack **highlights potential vulnerabilities** for systems that use networked industrial control systems and outdated operating systems

- It may also **inspire similar attacks** seeking to exploit such vulnerabilities at municipal water treatment plants

- Tampering with water treatment chemicals, by either increasing or decreasing the concentration delivered, could cause public health impacts

NIS directive

The **Directive on security of network and information systems** (NIS Directive) was adopted in 2016, and it provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- **Member States' preparedness**, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority

- **Cooperation among all the Member States**, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States

- **a culture of security across sectors** that are vital for the economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, and healthcare

Revised NIS directive (NIS 2 directive)

- **Greater capabilities**

o More stringent supervision measures and enforcement are introduced

o A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established

- **Cooperation**

o Establishment of European **Cyber crises liaison** organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

o Increased **information sharing** and **cooperation** between Member State authorities

o Coordinated **vulnerability disclosure** for newly discovered vulnerabilities across the EU is established

Revised NIS directive (NIS 2 directive)

Cybersecurity risk management

- Strengthened **security requirements** with a list of focused measures including **incident response** and **crisis management**, vulnerability handling & disclosure, etc

- Cybersecurity of **supply chain** for key information and communication technologies will be strengthened

- **Expanded scope to include more sectors** and services as either essential or important entities. E.g., **Waste water and waste management, Space**, etc

Cybersecurity framework

The **NIST Cybersecurity Framework** (NIST CSF) provides a policy framework of cybersecurity guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks

- Version 1.0(1.1) was published by the US NIST in 2014(2018), originally aimed at **operators of critical infrastructure**

- It can be used by a wide range of businesses and organizations, and helps shift organizations to be **proactive about risk management**
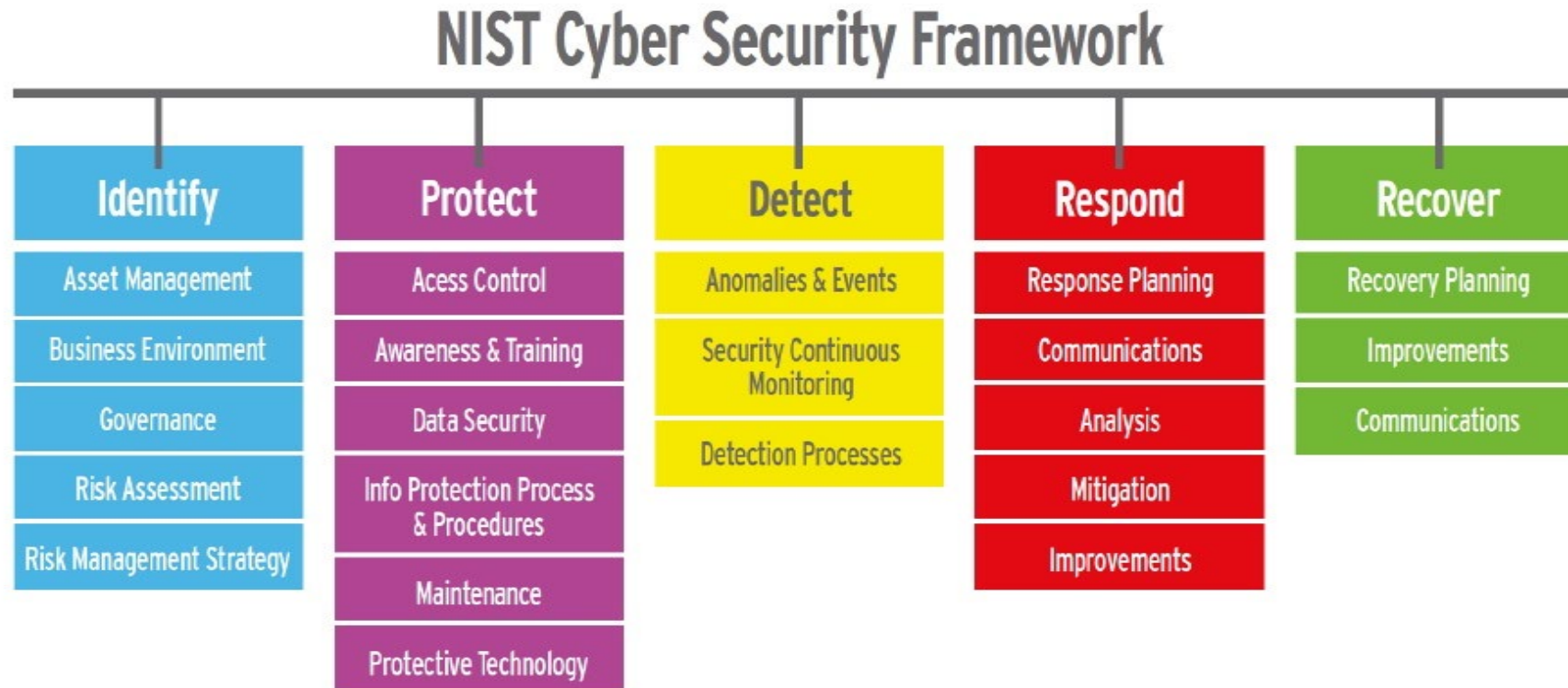
Cybersecurity framework

The Framework provides a common taxonomy and mechanism for organizations to:
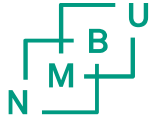
- Describe **current** cybersecurity posture

- Describe **target state** for cybersecurity

- Assess **progress** towards target state

- Communicate among internal and external stakeholders about cybersecurity risk

Cybersecurity framework

- **Identify**: develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

- **Protect:** develop and implement appropriate safeguards to ensure delivery of critical services

- **Detect**: develop and implement appropriate activities to identify the occurrence of a cybersecurity event

- **Respond**: develop and implement appropriate activities to take action regarding a detected cybersecurity incident

- **Recover:** develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity inciden

Cybersecurity framework

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Acess Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Process & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Basic security measures to reduce vulnerabilities & attacks

- Keep an inventory of control system & reduce exposure

- Segregate networks and apply firewalls

- Use secure remote access methods

- Establish roles to control access levels and log users

- Require strong passwords & password management

- Avoid vulnerabilities, implement patches, updates

- Enforce policies on the security of mobile devices and cyber security training program

- Involve utility executives in cyber security

- Monitor network intrusions and have a response plan

- Use <u>defense</u>-in-depth strategies

Defense in Depth Strategy Elements	
Risk Management Program	· Identify Threats · Characterize Risk · Maintain Asset Inventory
Cybersecurity Architecture	· Standards/ Recommendations · Policy · Procedures
Physical Security	· Field Electronics Locked Down · Control Center Access Controls · Remote Site Video, Access Controls, Barriers
ICS Network Architecture	· Common Architectural Zones · Demilitarized Zones (DMZ) · Virtual LANs
ICS Network Perimeter Security	· Firewalls/ One-Way Diodes · Remote Access & Authentication · Jump Servers/ Hosts
Host Security	· Patch and Vulnerability Management · Field Devices · Virtual Machines
Security Monitoring	· Intrusion Detection Systems · Security Audit Logging · Security Incident and Event Monitoring
Vendor Management	· Supply Chain Management · Managed Services/ Outsourcing · Leveraging Cloud Services
The Human Element	· Policies · Procedures · Training and Awareness

References

- Do etal, *Security of SCADA systems against cyber–physical attacks*, 2017

- NIS Cooperation Group, *Cybersecurity incident taxonomy*, Jul 2018

- Tuptuk etal, *A systematic review of the state of cyber-security in water systems*, Jan 2021

- NIST, *Framework for improving critical infrastructure cybersecurity*, Apr 2018

- Department of Homeland Security, *Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies*, Sep 2016

- DIRECTIVE (EU) 2016/1148 of the European parliament & the council of the EU, *concerning measures for a high common level of security of network & information systems across the Union*, Jul 2016

Thank you!