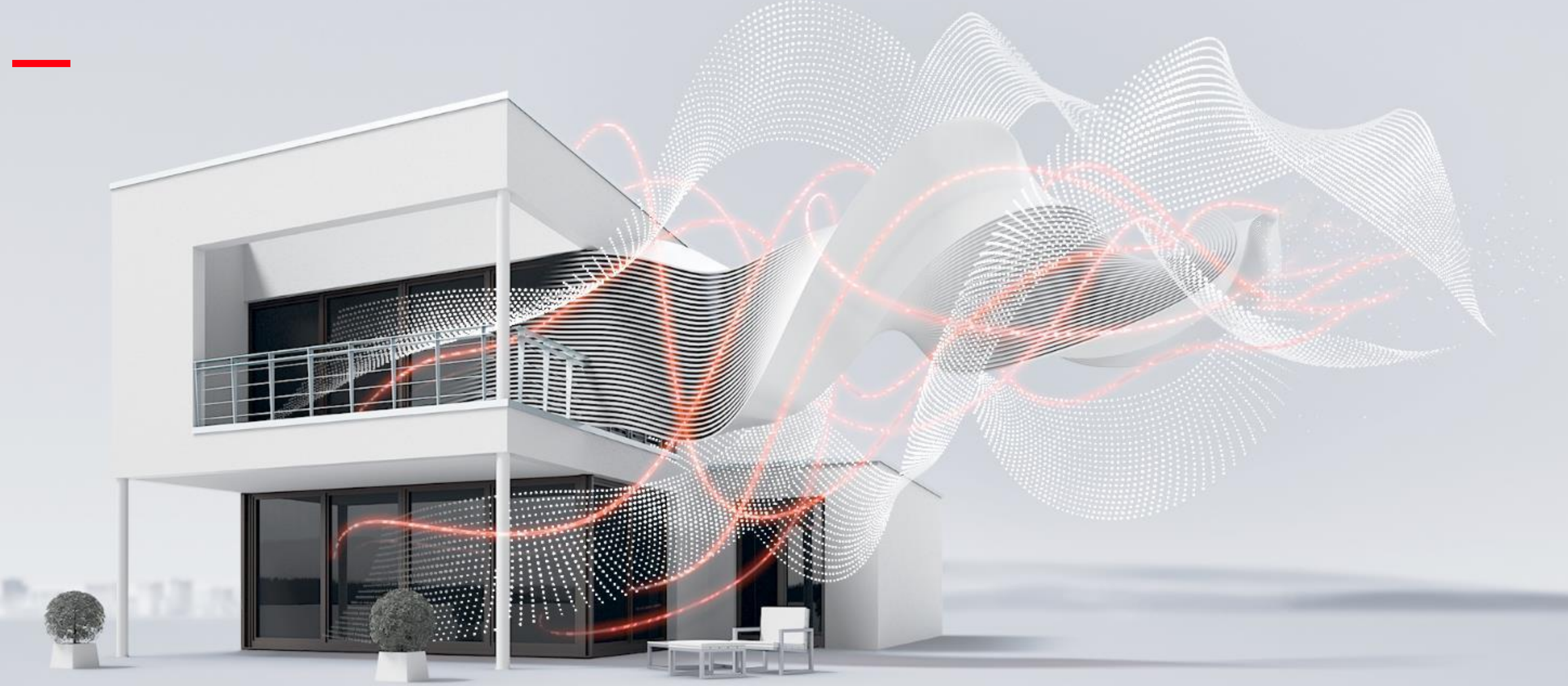


2020

ABB Ability Cyber Security Services

Life Cycle Management

Energy Industries

Guiding Principles

There are no Silver bullets…

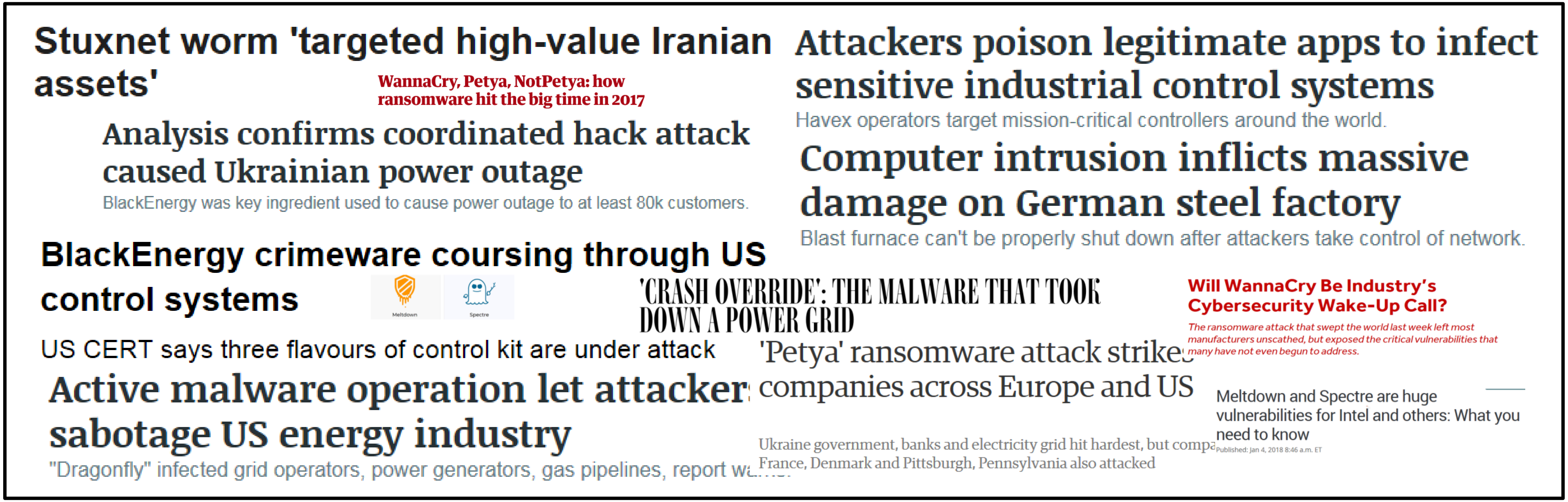
Reality	There is no such thing as 100% or absolute security
Process	Cyber security is not destination but an evolving target – it is not a product but a process
Balance	Cyber security is about finding the right balance – it impacts usability and increases cost

"Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."

Cyber security is all about risk management

Cyber Security in Power and Automation

This is not “fake news”…



Stuxnet worm 'targeted high-value Iranian assets'

WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Analysis confirms coordinated hack attack caused Ukrainian power outage

BlackEnergy was key ingredient used to cause power outage to at least 80k customers.

BlackEnergy crimeware coursing through US control systems

Meltdown
Spectre

US CERT says three flavours of control kit are under attack

Active malware operation let attacker sabotage US energy industry

"Dragonfly" infected grid operators, power generators, gas pipelines, report wa...

Attackers poison legitimate apps to infect sensitive industrial control systems

Havex operators target mission-critical controllers around the world.

Computer intrusion inflicts massive damage on German steel factory

Blast furnace can't be properly shut down after attackers take control of network.

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

'Petya' ransomware attack strike companies across Europe and US

Ukraine government, banks and electricity grid hit hardest, but compa France, Denmark and Pittsburgh, Pennsylvania also attacked

Will WannaCry Be Industry’s Cybersecurity Wake-Up Call?

The ransomware attack that swept the world last week left most manufacturers unscathed, but exposed the critical vulnerabilities that many have not even begun to address.

Meltdown and Spectre are huge vulnerabilities for Intel and others: What you need to know

Published: Jan 4, 2018 8:46 a.m. ET

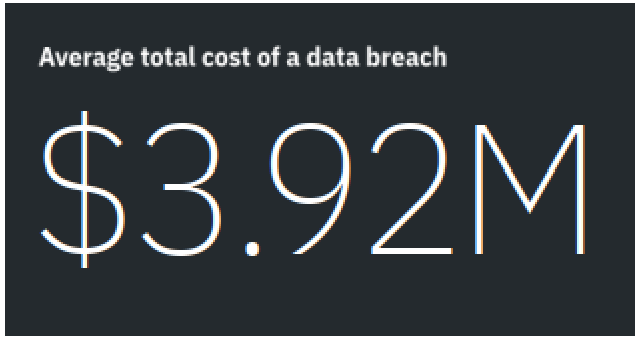
Attacks are real and have an actual safety, health, environmental, and financial impact

Cyber Security

..if not - cost of Cyber Crime

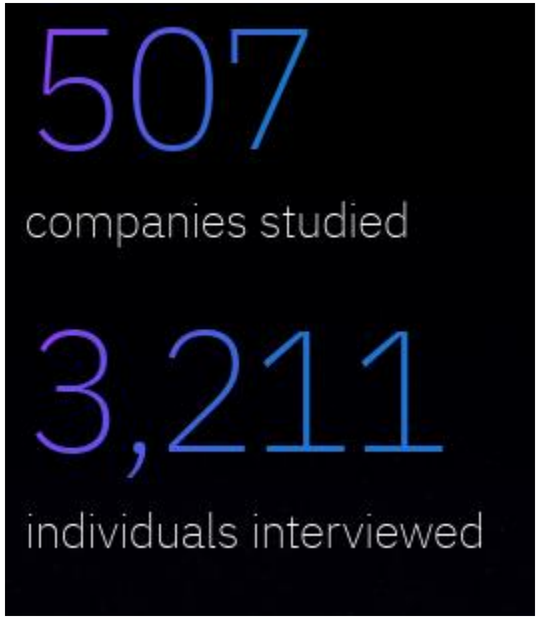
Global study 2019

- Lost of business was the biggest contributor to data breach costs
- Data breach costs impact organizations for years
- The lifecycle of data breach was longer
- Malicious attacks were the most common and expensive root cause



Average total cost of a data breach

$3.92M

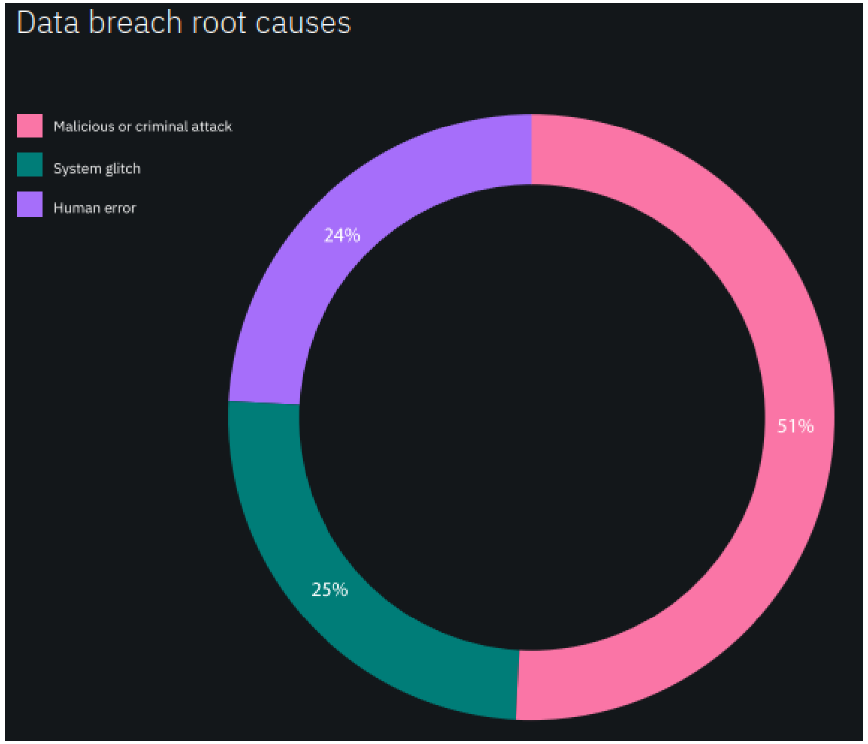


507

companies studied

3,211

individuals interviewed



Source: Ponemon Institute – Cost of a Data Breach Report 2019

Cyber Security

..if not -> typical findings

- Cyber crimes continue to rise for organizations
- Cyber crime cost varies by organizational size
- All industries fall victim to cybercrime, but to different degrees
- The most costly cyber crimes are those caused by malicious insiders, denial of services and web-based attacks
- Cyber attacks can get costly if not resolved quickly
- Business disruption represents the highest external cost, followed by the costs associated with information loss
- Deployment of security intelligence systems makes a difference

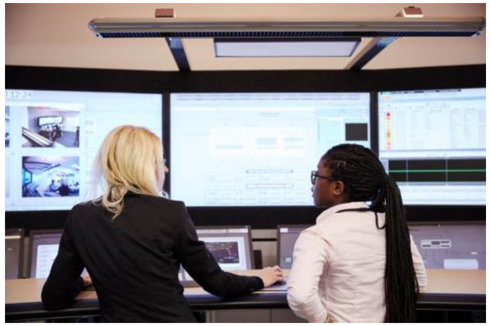
Our Current Cybersecurity Landscape

There is a hacker attack every 39 seconds

A recent study[1] quantified that there is a near-constant rate of hacker attacks. Non-secure usernames & passwords give hackers a higher chance of success.

Large-scale DDoS attacks increase in size by 500%

According to a 2018 report[3], the average distributed denial of service (DDoS) attach grew to over 26Gbps, increasing in size by 500%



The average cost of a data breach in 2020 will exceed $150 million.

As we increase connectivity to our business and critical infrastructure, data suggests that cyber crime will cost over $2 billion total in 2019.[2]

By 2020 there will be roughly 200 billion connected devices.

The number of IoT and IIoT devices is growing and so is the risk.

"Cyber crime is the greatest threat to every company in the world."[4]

Source: 15 Alarming Cyber Security Facts and Stats, Cybint Solutions, September 23, 2019

[1] University of Maryland Clark School study

[2] Juniper Research

[3] Q2 2018 Threat Report, Nexusguard

[4] Ginni Rometty, IBM Chairman, President and CEO

There are no magic solutions; security maturity takes time

Must engage and educate people, develop and deploy processes, and design and deliver protected technology

3 Cyber objectives:

- People, Process and Technology: each must be leveraged to protect digital systems

People

- People are critical in preventing and protecting against cyber threats.
- Organizations need competent people to implement and sustain cyber security technology and processes.

Process

- Policies and Procedures are key for an organization's effective security strategy.
- Processes should adapt to changes as cyber threats evolve.

Technology

- Technology is important in preventing and mitigating cyber risks.
- Technology needs people, process and procedures to mitigate risks.

Pain points

Current challenges and changes

Increased ICS Cyber Threats

STUXNET, BLACKENERGY, HAVEX, CRASHOVERRIDE, TRISIS, WannaCry.

Few people understand how to protect our control systems

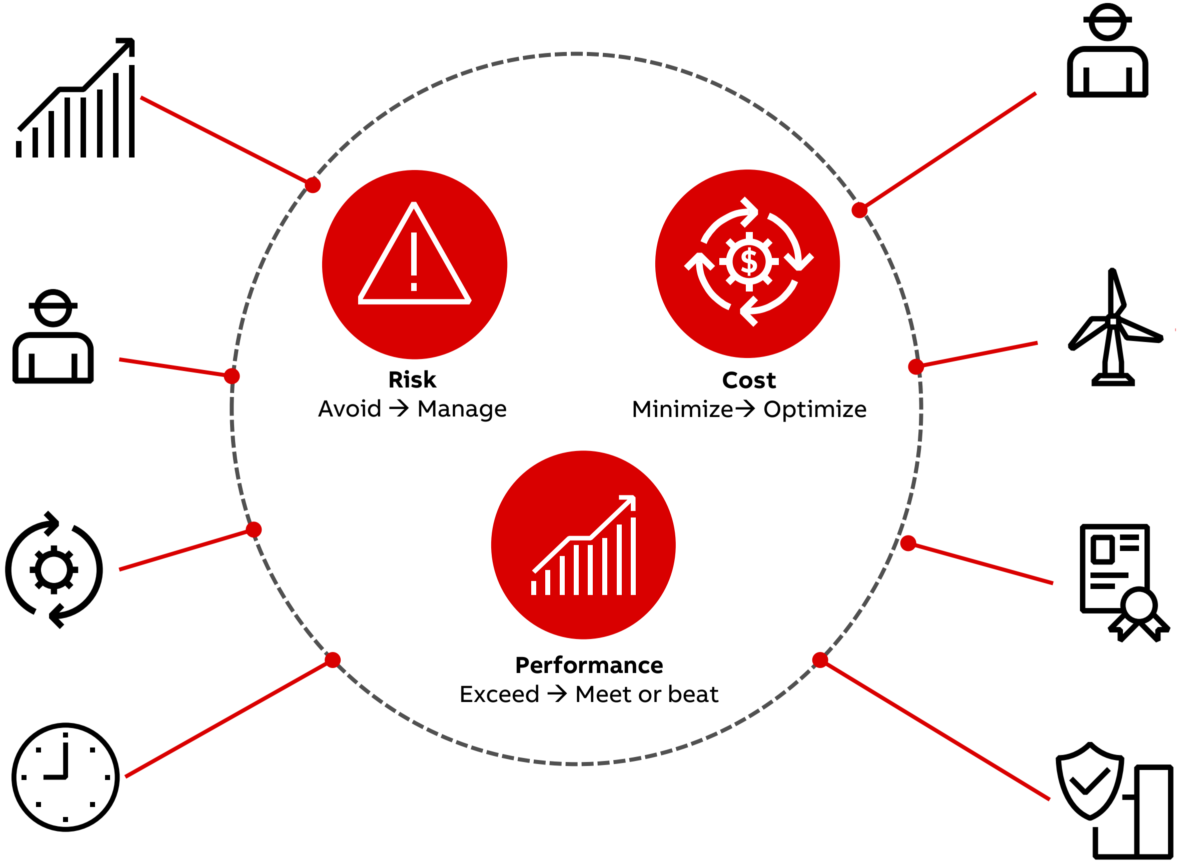
We need more experts in both Operational Technology and Cyber Security.

IT/OT convergence

CISOs require OT systems to following corporate security standards for patching, anti-virus and monitoring.

Desire to extend the life span

Industrial control systems are running on EoL software with known vulnerabilities. Operators are looking for ways to extend the life.



Risk
Avoid → Manage

Cost
Minimize→ Optimize

Performance
Exceed → Meet or beat

Workforce focusing on high-value tasks

Organizations scaling back on dedicated headcount, limited resources need to focus on higher value activities - looking for ways to automate sustaining secure systems.

Distributed assets difficult to secure

Assets are becoming more intelligent and distributed, the attack surface is expanding making it difficult to protect with traditional approaches.

Compliance with industry standards

HSE Compliance example

Lack of situational awareness tools

ICS asset owners have no visibility into the security posture and status. Monitoring cyber security across operational assets is difficult to implement.

ABB Ability Cyber Security Services

Simplified security solutions

Foundation

Assessment

Assessments are solutions that measure gaps in your system compared to a defined best practice. The best practice can be industry standards, customer policies, or ABBs recommendations as a control system vendor.

Security Controls

A set of cybersecurity products delivered as software as a service (SaaS) running on a computers or servers connected to your production system or directly on your computers in the control system. It is expected that the customer manages the solution after ABB installs and configures it. ABB is responsible for updates and the general availability of the system.

Training

ABB University – Training center that provides comprehensive training for ABB systems, services, maintenance and operation.

Services

Maintenance

Any software nowadays is exposed to security analysis by security experts (both with good and bad intentions). This often results in vulnerabilities being discovered. Our services includes continuous lifecycle maintenance of cyber security for your control systems and approval of 3rd party security patches for ABB control systems, giving you the comfort of knowing that your system is always on an up-to-date level.

Consulting

Some of our customers have special needs for cyber security support. ABB can offer customized consulting services where our cyber security specialists will be available for support.

Operations

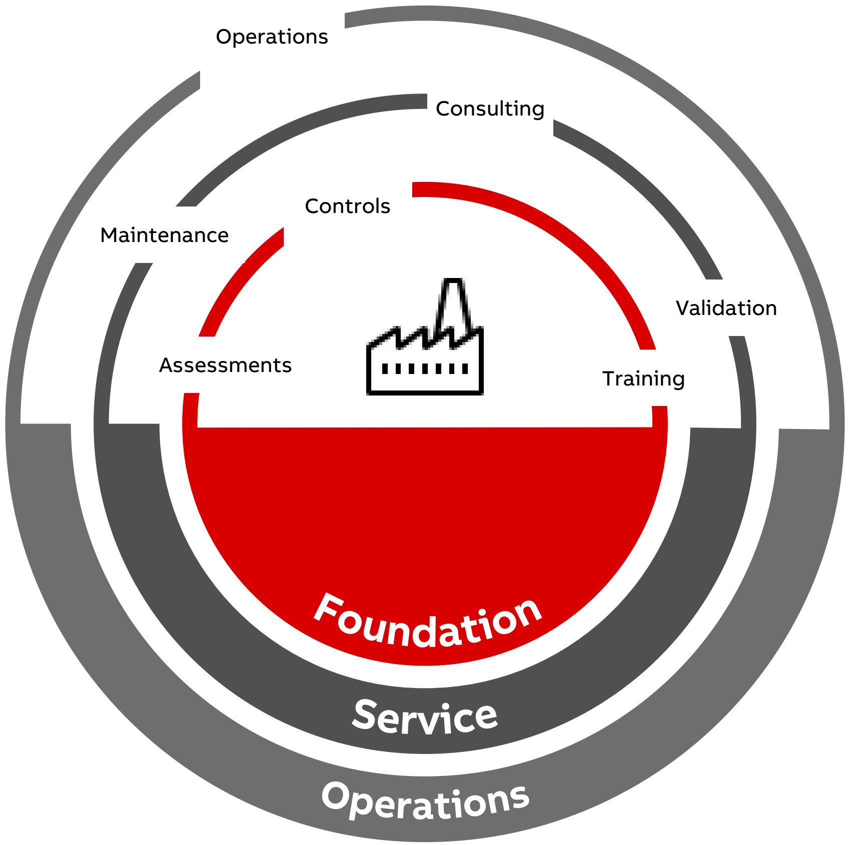
Collaborative Operations

ABB Security Operation Center (SOC) is a centralized function within our organization employing people, processes, and technology to continuously monitor and improve our customers production systems security posture while preventing, detecting, analyzing, and responding to cyber security incidents.

The function of a security operations center, is to monitor, detect, investigate, and respond to cyberthreats around the clock. ABB's security operation team is charged with monitoring and protecting production system assets, such as intellectual property, applications, control systems, and brand integrity. Our security operations teams act as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks.

ABB Ability Cyber Security Services

Value added System Integrator -> 3 Pillar Operational Services Journey



🟥 **Foundation** - Transactional Integration services *(Security Controls & Reference Architecture)*

■ **Services** - Contractual Maintenance services *(CARE contract)*

■ **Operations** - Contractual Operational services *(Monitoring, Incident Response, Cyber Physical Analytics)*

ABB Ability^{TM} Cyber Security Services

Case studies

Chemical plant in West Virginia, USA mitigates risk with ABB Cyber Security Fingerprint

DTE Energy in Michigan, USA mitigates risk with ABB Cyber Security, Harmony and System 800xA Fingerprints

Goliat - Delivering the world's most integrated and digitally-enabled off-shore plant

Northern European TSO Enlists ABB to keep the lights on and fend off cyber-attacks

Enhancing cyber security with incremental upgrade to latest version of System 800xA

European steel mill mitigates risk with ABB Cyber Security Fingerprint

Photo credit: BASF SE

BASF rotating machine digital service

Söderenergi in Sweden digitizes manual and automated tasks using ABB remote monitoring

storaenso

Stora Enso, a provider of packaging, wood and paper, chooses ABB for cyber security

Middle eastern refinery tightens security with ABB Cyber Security Fingerprint

Norske Shell uses ABB's automation technologies at their oil and gas fields at Draugen and Ormen Lange

Sadara - Enabling the world's largest petro-chem complex built in one phase

Multi-national gas supplier thwarts cyber attackers with ABB Ability™ System 800xA v6 and ABB Security Update Service

Queensland Curtis LNG facility in Australia uses ABB's digital infrastructure to achieve higher efficiencies

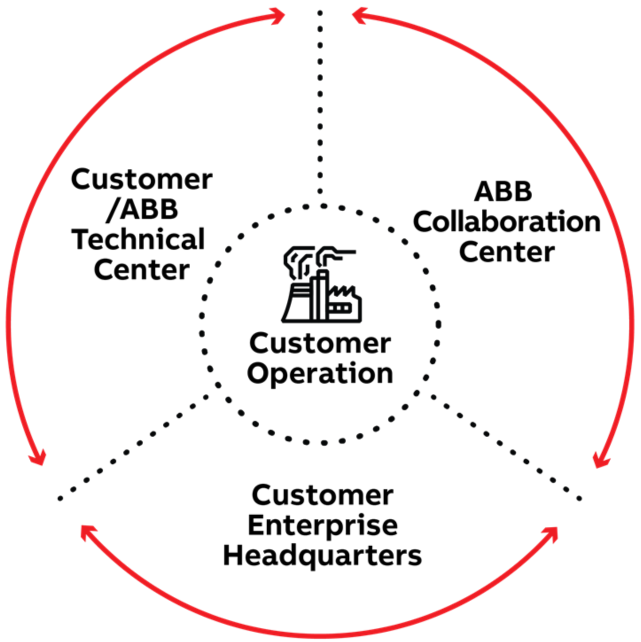
Boliden in Sweden mitigates risk with ABB Cyber Security Fingerprint

https://new.abb.com/process-automation/case-studies/cyber

Our customers want to connect and transform

Local operating companies, single plants, regional headquarters, and enterprise headquarters

Remotely collaborating with our customers globally



Customer /ABB Technical Center

ABB Collaboration Center

Customer Operation

Customer Enterprise Headquarters

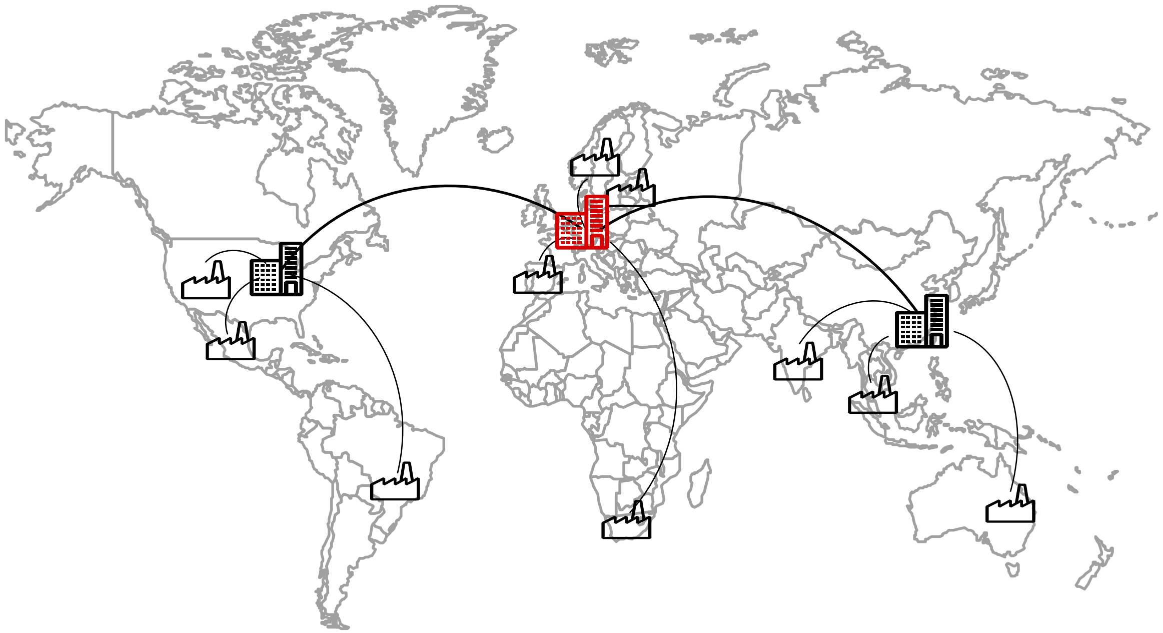


ABB Collaborative Operations

Benefits

- Safe remote operations from ABB Collaborative Operation Center
- Continuous collaboration and access to experts
- Fast incident response
- Improved communication between you and ABB
- Increased uptime and lower cost – avoiding shut downs /ensure more stable operation
- 15 years experience with operator partnership
- Compliance with international standards
  - ISA/IEC 62443

ABB is actively participating in establishing best practices as part of international industry standards

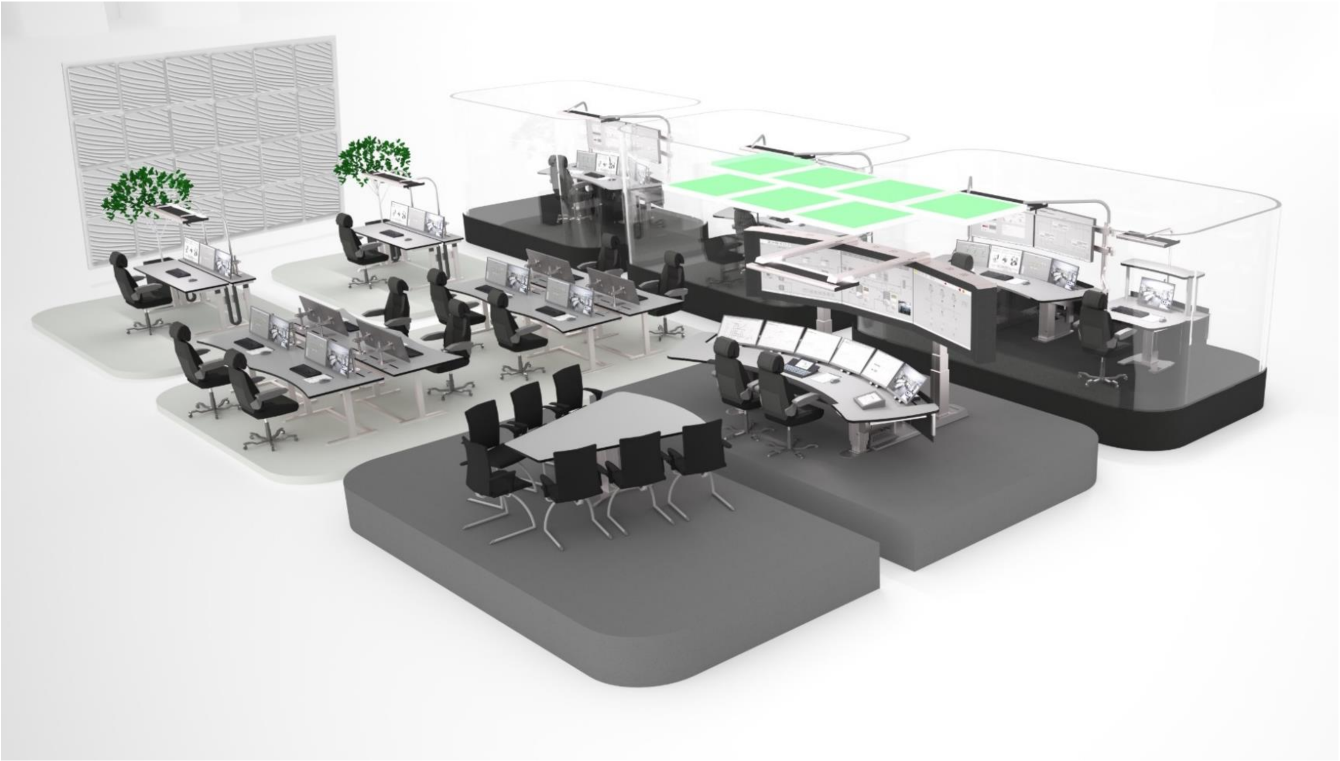


ABB Ability Cyber Security Services

Value proposition

Customer’s peace of mind

Safety and integrity

- Enhances risk mitigation against a cyber security attack
- Improves system availability
- Increases plant protection
- Improves production and equipment uptime
- Helps ensure compliance with international standards and customer’s internal security policy

ABB Ability Cyber Security Services

Contact information

https://new.abb.com/contact/form/#

https://new.abb.com/contact-centers

ABB