ABB Ability Cyber Security Services

Life Cycle Management

Oil & Gas and Chemicals
**Guiding Principles**

There are no Silver bullets…

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

“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'
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
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 says.

Attackers poison legitimate apps to infect sensitive industrial control systems
Hавекс 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.

Attacks are real and have an actual safety, health, environmental, and financial impact
This year the study conducted interviews with more than 2,200 IT, data protection, and compliance professionals from 477 companies in 15 countries that have experienced a data breach over the past 12 months. According to the findings, data breaches continue to be costlier and result in more consumer records being lost or stolen, year after year.

- The average total cost rose from $3.62 to $3.86 million, an increase of 6.4 percent
- The average size of the data breaches in this research increased by 2.2 percent

Source: Ponemon Institute – 2018 Cost of a Data Breach Study
Impact of cyber attacks on critical infrastructure

Cyber exploits on OT disrupting the standard of living

Cyber attacks cost $300 million of profits
One of the world’s biggest container shipping companies, A.P. Moller-Maersk A/S reported the loss in their third quarter financial report.

OT cyber security state of readiness
66% of organizations are not ready to address security issues for OT
61% of organizations in oil & gas believe it’s unlikely they would be able to detect a sophisticated attack

Increasing trend of cyber attacks
67% of companies with critical infrastructure suffered at least one attack in the past 12 months

Future predictions
78% expect a successful exploit of their ICS/SCADA systems within the next two years

Hackers are deliberately selecting targets, including industrial control systems used by power plants

---

1 Critical Infrastructure: Security Preparedness and Maturity (July 2014), Unisys and Ponemon
2 2015 Global Megatrends in Cybersecurity, Raytheon and Ponemon
3 Oil and Gas Cyber Security: Time for a Seismic Shift, 2015, EY
4 Excerpt from the article “Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns”, published in Bloomberg, March 15, 2018
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
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 Pillars:

– 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.

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.
# How can ABB help our customers?

## Complete life cycle of protection

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond &amp; Recover</th>
<th>Consulting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know where to fix</td>
<td>Know how and what to fix</td>
<td>Ability to detect</td>
<td>Ability to help</td>
<td>Ability to consult</td>
</tr>
<tr>
<td>First identifying what needs to be protected</td>
<td>Implement and maintain security solutions for protection</td>
<td>Monitor to notify breaches and vulnerabilities</td>
<td>Respond to help and restore if compromised</td>
<td>Support with expertise</td>
</tr>
<tr>
<td>Perform assessments and collect inventory to identify what needs to be protected.</td>
<td>Provide validated updates, maintenance and implement custom configured solutions for endpoint protection.</td>
<td>Monitor system to detect breaches and vulnerabilities. Collect and analyze security logs.</td>
<td>Execute incident response exercises to prepare for an incident if compromised. Reduce impact of incident by recovering quickly.</td>
<td>ABB can provide training, compliance services, strategy / policy creation, and vulnerability testing.</td>
</tr>
</tbody>
</table>

We will deliver cyber security services across ABB’s scope of supply AND across our customers’ fleet.
# ABB Cyber Security

Complete life cycle portfolio for each step in the journey

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
<th>Respond &amp; Recover</th>
<th>Consulting</th>
</tr>
</thead>
<tbody>
<tr>
<td>First identifying what needs to be protected</td>
<td>Implement and maintain security solutions for protection</td>
<td>Monitor to notify breaches and vulnerabilities</td>
<td>Respond to help and restore if compromised</td>
<td>Support with expertise</td>
</tr>
</tbody>
</table>

### Solutions
- **Identify**
  - Cyber Asset Inventory
  - Cyber Security Fingerprint

- **Protect**
  - Malware protection
  - Security patch updates
  - System hardening
  - Backup and recovery
  - User and access
  - Reference Architecture

- **Detect**
  - Security event monitoring (SIEM Solution)
  - Security analytics

- **Respond & Recover**
  - Incident response plan
  - Recovery testing

- **Consulting**
  - Organized cyber security service teams

### Services
- **Identify**
  - Cyber Security Risk Assessment
  - Cyber Security Assessment

- **Protect**
  - Cyber Security lifecycle maintenance

- **Detect**
  - Collaborative Operations

- **Respond & Recover**
  - Incident Response
  - Disaster recovery

- **Consulting**
  - Training
  - Strategy and Policy
  - Compliance

### Compliance
IEC 62443, ISO27000, NIST, NIS Directive, NERC CIP.
Identify your Vulnerabilities

Cyber Security fingerprint

**Procedures and protocols:** Qualitative analysis that indicates how secure the organization is by the means of written instructions and policies.

**Group security policies:** Policies implemented on the system, enforced from a central server or implemented on an individual computer.

**Computer settings:** Settings and applications that reside on individual computers in the system.
Identify your Assets

Cyber Security Asset Inventory

- Identify all your assets, zones and conduits.
- Identify vulnerable assets, insecure device configurations
- Identify suspicious devices
- Automatically generate reports related to asset inventory

Key deliverables: Simple Network Diagram, Asset Register.
Identify your Risks

Cyber Security Risk Assessments

- Describe the devices covered by the assessment
- Describe the threats (Phishing, Ransomware, Disgruntled Employee)
- Classify and prioritise the risk
- Make decisions on security controls

Key deliverables: identify, analyze and evaluate risk
Identify your security controls

Cyber Security Assessment

- Gathering data from control systems environment
- Security review of control system assets and infrastructure
- Give recommendations
- Make decisions on security controls
- Design a security plan for implementation

Key deliverables: assess, plan and design for implementation
Implement Security Controls

Use the Risk Assessment to identify which security controls require implementing:

- Device Hardening
- Malware protection
- Security Patch updates
- Backups and Recovery
- User and Access management
- Network Security
- Cyber Security Training
Detect any intrusions

Cyber Security Event Monitoring

– Collect your data
  • Syslogs
  • Firewall Logs
  • Netflow data

– How to detect malicious activity
  • Threat Intelligence
  • Anomaly detection

Do you have the ability to detect?

61% of oil and gas organizations believe it’s unlikely or highly unlikely that they would be able to detect a sophisticated attack*

Incident Response and Recovery

Things to consider:

- Roles and Responsibilities
- Incident Response plan
- Communications with media, customers, law enforcement, government and vendors
- Post incident forensics
- Exercising your plan
- Recovery and restoration

* 6% of Oil & Gas companies have a robust incident response program and regularly conduct table-top exercises.*

ABB Consulting Services can advise you and help you with planning or streamlining your deployment, upgrades, or evaluating, managing and maturing your security posture, we provide unrivaled experience, expertise and industry intelligence.

Security compliance checks and training to on-site residency services. ABB consultants work with you to pull the maximum value and protection from your cyber security investment.
Case studies

ABB Ability™ Cyber Security Services

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

Goliath - Delivering the world’s most integrated and digitally-enabled offshore plant

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

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

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

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

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

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

European steel mill mitigates risk with ABB Cyber Security Fingerprint

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

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

Boliden in Sweden mitigates risk with ABB Cyber Security Fingerprint

https://new.abb.com/process-automation/case-studies/cyber
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*
Our customers want to connect and transform
Local operating companies, single plants, regional headquarters, and enterprise headquarters

Remotely collaborating with our customers globally
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
Oil & Gas and Chemicals