ABB Ability™ Cyber Security Services
Protection against cyber threats takes ability
In today’s business environment, cyber security is critical for ensuring reliability of automation and control systems.

ABB Ability™ Cyber Security Services mitigate cyber risks by identifying potential threats, automating compliance efforts and defending against cyber-attacks.
Cyber threats are real and every industry is facing increased risk of cyber-attacks. Malicious attacks have caused losses of hundreds of millions of dollars to companies globally, and threat actors continue to find new ways to attack information and operational systems. To protect assets, processes and people from this imminent danger, companies must develop a cyber security strategy, and integrate cyber security measures into their processes.

### Cyber-attacks companies are most likely to face

- **Socially engineered threats** → End-user is tricked into installing a malicious program
- **Phishing attacks** → Skillfully crafted email in which a user clicks on a link or attachment, from which an attack is launched.
- **Unpatched software** → Vulnerabilities found in operating systems that have not been patched
- **USB and other removable media** → Personnel passing security controls such as airgaps, firewalls and data diodes
- **Advanced Persistent Threats (APT)** → Sophisticated exploits designed to go undetected, leveraging undisclosed system vulnerabilities

### Adopt a defense-in-depth strategy

Many attacks are successful because the virus or malware can quickly move across the network from one host to another using credentials from one asset. To minimize the impact of these attacks, it is important to have multiple layers of cyber security protection.
Strengthen security with a complete portfolio of cyber security solutions

—

ABB provides a range of cyber security solutions that minimize cyber risks and provide the highest level of protection for automation assets. We work with our customers to:

1. **Identify** areas in automation that may be vulnerable to cyber-attacks.
2. **Protect** assets by segmenting, hardening and implementing necessary controls.
3. **Detect** security breaches and vulnerabilities to predict and prevent unwanted incidents.
4. **Respond** on-demand to a cyber-attack that compromises systems.
5. **Recover** faster from a cyber event with a maintained backup system in place, complete with recovery feature.

ABB addresses cyber security at each phase of an automation asset’s life cycle, from design and development to operations and maintenance. We work with our customers to develop processes that ensure the highest level of protection for all automation assets against cyber-attacks and security breaches. We follow a process that includes identifying what must be protected, actively protecting the automation assets, detecting security breaches, responding to cyber-attacks and establishing backup and recovery plans. We also work with our customers to restore systems and recover information in case they are impacted.
Why ABB Ability™ Cyber Security Services

We bring three key areas of expertise:

Technology

ABB pioneered the development of electrical and automation technologies, and has years of experience helping customers protect control systems and other automation assets. Our cyber security solutions are aligned with industry standards and go through rigorous testing before they are released.

Industry Knowledge

ABB’s control systems are present globally across many industries. We know the type of cyber threats our customers face and what needs to be done to mitigate risks. We stay ahead of threats by investing heavily in research and development to continuously improve our security offerings.

Analytics

ABB has been helping customers become more cyber-secure through strong data analytics and visualization. Our technology identifies, categorizes and prioritizes Key Performance Indicators (KPIs) automatically, so our experts can determine the best risk mitigation strategies.

Case Studies

Steel mill, Spain

Needed to review control system cyber security status and ensure software and antivirus programs were up-to-date.

We met that need with ABB Ability™ Cyber Security Fingerprint

Customer Benefit

Helped to reduce vulnerabilities and develop a lasting security strategy.

Specialty chemical facility, USA

Needed to assess the potential exposure to computer viruses and malware.

We met that need with ABB Ability™ Cyber Security Fingerprint

Customer Benefit

Mitigated risk against a cyber security attack and established an ongoing security plan.

Pulp and paper mill, Germany

Needed to improve cyber security measures for mitigating cyber risks and ensuring compliance with European Union’s security standards.

We met that need with ABB Ability™ Cyber Security Analytics

Customer Benefit

Reduced vulnerabilities and provided a sustainable security strategy for mill’s control systems.
Help us meet your cyber security needs

**IDENTIFY**

1. Do you believe that your operational technology systems are protected from cyber risks?
   - O Yes
   - O No
   - O Not sure

2. Do you have a comprehensive list of cyber assets?
   - O Yes
   - O No
   - O Not sure

**ABB ABILITY™ CYBER SECURITY BENCHMARK**

Know your organization’s cyber security status through a simple easy-to-read color-coded stoplight report.

**ABB ABILITY™ CYBER SECURITY FINGERPRINT**

Take a deeper dive into your organization’s cyber security status with a report that provides detailed recommendations for reducing cyber security vulnerabilities.

**ABB ABILITY™ CYBER SECURITY ASSESSMENT**

Get detailed security information on control system infrastructure and existing cyber security measures with this in-depth site survey.

**ABB ABILITY™ CYBER SECURITY RISK ASSESSMENTS**

Improve security of your automation control systems by performing a threat/risk-based assessment.

**ABB ABILITY™ CYBER ASSET MANAGEMENT**

Ensure complete protection by creating and maintaining an accurate inventory of automation assets within the operational environment.

**PROTECT**

3. Does your company have an operational technology cyber security program in place?
   - O Yes
   - O No
   - O Not sure

4. What is the frequency for applying security patches to your operational systems?
   - O Monthly
   - O Never
   - O Quarterly
   - O Yearly
   - O Not sure

5. Have your operational technology systems been isolated from other networks?
   - O Yes
   - O No
   - O Not sure

6. Does your organization remove outdated software and unused user accounts on a regular basis?
   - O Yes
   - O No
   - O Not sure

**ABB ABILITY™ MALWARE PROTECTION MANAGEMENT**

Ensure effective protection from malware by having protective technology deployed on end-point assets.

**ABB ABILITY™ SECURITY PATCH MANAGEMENT**

Reduce the likelihood of a cyber-attack by regularly implementing software patches on automation systems.

**ABB ABILITY™ SYSTEM HARDENING**

Reduce the risk of a cyber-attack by decreasing the size of potential attack surface.

**ABB ABILITY™ USER AND ACCESS MANAGEMENT**

Make your systems more secure by establishing and clearly defining access permissions.
7. Do you have a process to monitor your system for published vulnerabilities?
O Yes  O No  O Not sure

8. Do you have a process to ensure cyber security for your entire fleet of automation assets?
O Yes  O No  O Not sure

9. Have you considered network segregation to contain the impact of a breach or attack?
O Yes  O No  O Not sure

---

**ABB ABILITY™ CYBER SECURITY ANALYTICS**
Get actionable information on the security status of your control systems in a simple web-based dashboard.

**ABB ABILITY™ CYBER SECURITY MANAGEMENT**
Monitor and sustain security controls across your fleet of automation and control assets.

**ABB ABILITY™ NETWORK SECURITY MANAGEMENT**
Secure the system’s perimeter and the internal network within the system’s architecture.

---

10. Do you have a plan in place to respond to a cyber-attack?
O Yes  O No  O Not sure

---

**ABB ABILITY™ INCIDENT RESPONSE**
Get end-to-end support during and after a security incident.

---

11. Do you have a plan in place to help you recover from a cyber-attack?
O Yes  O No  O Not sure

---

**ABB ABILITY™ SYSTEM BACKUP & RECOVERY MANAGEMENT**
Ensure that system failures or extended downtime do not cause loss of data.

---

**PLEASE SELECT YOUR INDUSTRY:**

O Cement  O Chemicals  O Data Centers  O Food & Beverage  O Manufacturing  O Marine

O Metals  O Mining  O Oil & Gas  O Pharmaceuticals  O Power Generation  O Pulp & Paper

O Water  O Other

---

Thank you for taking the time to help us identify your cyber security requirements. If you answered “no” or “not sure” to any of the questions, you are not alone. Protecting operational systems from cyber risks can be a challenge and requires methodical strategies and robust solutions.

ABB can help you implement and sustain cyber security solutions for your automation and control systems. To learn more, simply drop an email to automation.service@us.abb.com. Our representative will contact you soon.
Make your assets cyber-secure today  
To get started or learn more, please contact your local ABB sales representative or visit: 
— 
abb.com/cybersecurity