ABB Ability™ Cybersecurity services

Protection against cyber threats takes ability

In today's business environment, cybersecurity is critical for ensuring reliability of automation and analyzer networks.

ABB Ability™ Cybersecurity services mitigate cyber risks by identifying potential threats, automating compliance efforts and defending against cyber-attacks.

Protect your automation assets from cyber-attacks

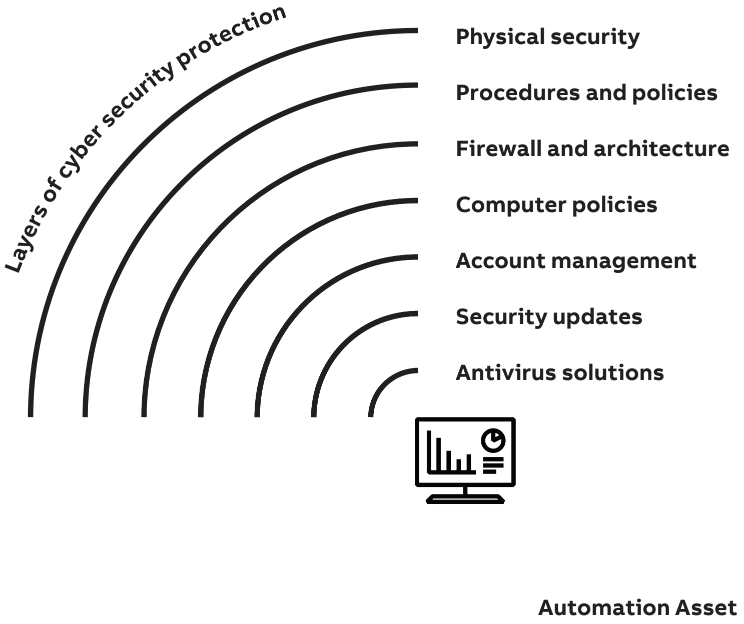
Cyber threats are real and every industry is facing increased risk of cyber-attacks. Malicious attacks have caused losses of hundreds of millions of dollars to companies globally, and threat actors continue to find new ways to attack information and operational systems. To protect assets, processes and people from this imminent danger, companies must develop a cybersecurity strategy, and integrate cybersecurity 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 cybersecurity solutions

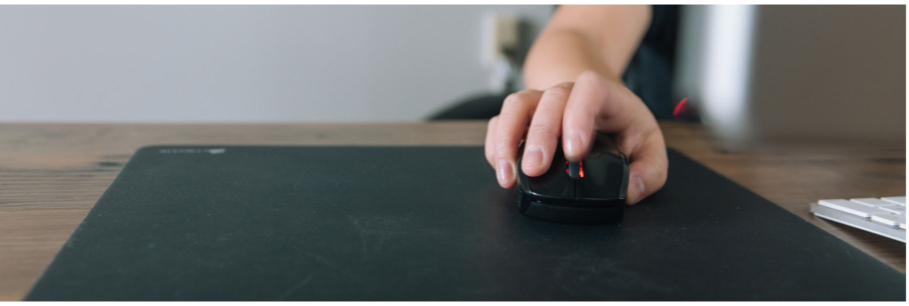
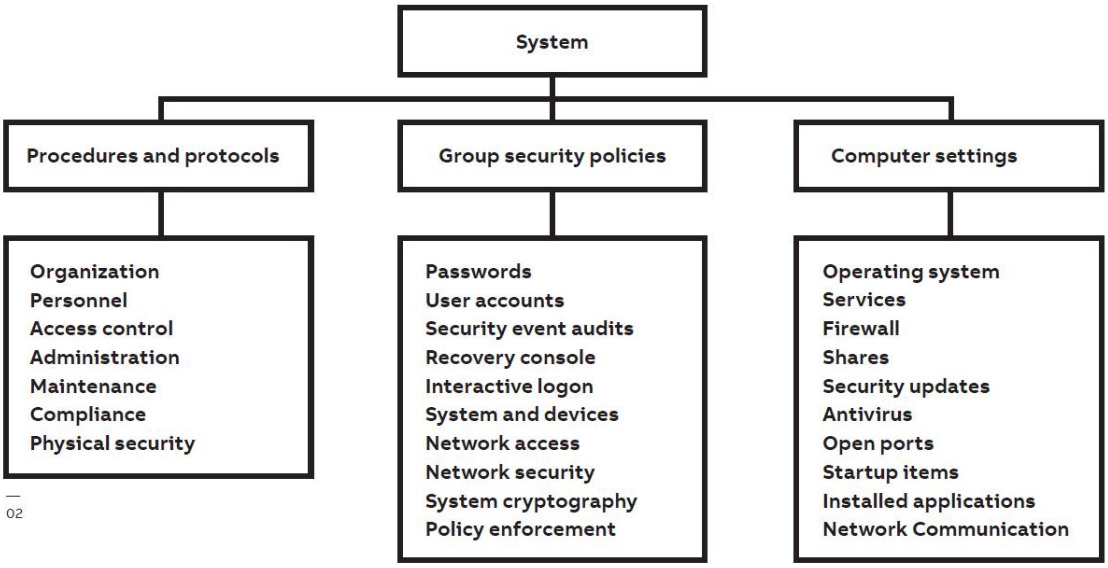


ABB provides a range of cybersecurity solutions that minimize cyber risks and provide the highest level of protection for automation assets & analyzer networks we work with our customers to:

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

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 cybersecurity 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.



System

Procedures and protocols

Organization
Personnel
Access control
Administration
Maintenance
Compliance
Physical security

Group security policies

Passwords
User accounts
Security event audits
Recovery console
Interactive logon
System and devices
Network access
Network security
System cryptography
Policy enforcement

Computer settings

Operating system
Services
Firewall
Shares
Security updates
Antivirus
Open ports
Startup items
Installed applications
Network Communication

—
02

Why is Cybersecurity important ?

What every customer needs to know

Modern automation, safety and analyzer network are highly specialized IT systems.

01 **Leverage commercial off the shelf equipment**

02 **Rely on the standard internet communication protocol**

03 **Are distributed and highly interconnected**

04 **Use mobile devices and storage media**

05 **Are increasingly connected to cloud platforms**

06 **Are highly based on software**

→ **Increased vulnerabilities as compared to legacy, isolated systems**

→ **Communication with IT systems, which facilitates attacks from / over the IT world**

Why Cybersecurity is important to ABB business?

Because of our customers!

ABB customers want:
To run their business in a safe, sustainable, reliable, and efficient way. While benefiting from technology advancements such as Digitalization, Industrial Internet of Things and Industry 4.0

-

ABB customers expect:
Top-level quality from ABB products, systems, engineering projects, and services – including how we deliver services and manage engineering projects – to ensure customers' safe, sustainable, reliable and efficient operations

Security is a significant component of quality:
Security is becoming a priority of our customers. Security shall become a priority for ABB

ABB Cybersecurity services
What we offer

OS Hardening

- Application
- Ports
- Services

Network Hardening

- Firewall rules
- Routing tables
- Switch hardening

Application Hardening

- User accounts
- User Context for applications
- Application and services executing with least privileges

Policies

- Definition of policies
- Policy deployment
- Policy enforcement
- Password policies

Antivirus & Malware protection | Back up & restore

Antivirus

- Antivirus solution
- Validated antivirus definition files
- Deployment of antivirus definition
- Keeping the antivirus definition up to date
- Vistatnet gateway
- Frequency

Back up & restore

- Define backup volume and frequency
- On-premise or external backup
- Test backup by performing restore exercises
- Restore when necessary

Logging

- Enabling logs
- Log aggregation
- Monitoring log files
- Analysis of logs
- Collecting event logs and send to a log aggregation server
- Provide dashboards for event viewing
- Monitoring and analysis of event logs for anomalous events
-
- **Patch management**
- Patch identification
- Patch qualification
- Patch deployment
- Infrastructure for patch management

Security updates
ABB will monitor the installed software and hardware components

Patching schedule

- Likelihood – has working code been published
- Exposure – are the vulnerable systems or services internet – accessible or open to entire org?
- Context – Severity? Complexity? Kind of impact? Ease of detection?
- Mitigation – are there verified workarounds which can be implemented until full patching can occur?

List of supported Operating Systems & Software

- “Supported” means system is receiving security updates if a system is deemed end-of-life by ABB, the unsupported software must be upgraded

General patching guidance – identify vulnerability, evaluate available patches, test and deploy patches, confirm successful installation

- Automate
- Plan & Prioritize
- Monitor

Account Management
Inspection & Assessment

Creation of active directory

- Migration of existing users in active directory
- Management of all systems using active directory

Role based access control

- Individual accounts only, no shared "Administrator" accounts or "built-in" accounts in normal use (Domain or Local Windows)
- No highly privileged "Administrator" or "Built-In" ac-counts "blank", "extremely weak" or "default" pass-words for windows and Application.
- Administrator rights to be removed from Application accounts (including database and service accounts) by assigning the correct access control and privileges in the right places, particularly in DCOM and on the file system.

Password Management

- Implement Minimum Password Strength (Standard 8 Characters, Application / Administrator 15 character). Minimum complexity of password should be Upper case letters, lower case letters, numbers, symbols
- No Blank, Weak or Default passwords in Domain/Windows/Linux.
- No Blank, Weak or Default passwords in System, database and applications, DCOM etc.
- Rename and disable local "Built-in" administrator and guest accounts.
- Forgotten password

Database Management