ABB ABILITY™ CYBER SECURITY SERVICES

Cyber Security Risk Assessment

Address your highest risks while maximizing productivity

- Better understand your cyber security risk
- Highlight the highest risk areas
- Identify steps to remediate risk

Industrial operators are increasingly aware of the potential for cyber-attacks, but few have the domain knowledge to address needs in house.

An ABB Cyber Security Risk Assessment helps plant operators and facilities managers uncover, rate, prioritize and remedy control system cyber security risks.

Armed with this knowledge, leadership can make the changes required to ensure cyber security readiness.

Stay ahead of bad actors with ABB.

Great benefits mean great vulnerabilities
Addressing risk in a changing market

The current digital environment

Operational Technology (OT) has become increasingly connected, and the integration of Information Technology (IT) components allows such devices to leverage software that drives data collection and analysis, resulting in enhanced performance and ultimately "smarter" machines. With these benefits come vulnerabilities, including the possibility of malicious actors gaining access to critical assets through networks. The growing recognition of cyber security threats to critical infrastructure (e.g. energy, water, transportation) has brought the topic into the spotlight.

Challenges

Regulatory alignment
Companies are required to perform and document cyber security assessments on a regular basis by regulatory requirements such as IEC 62443.

Effective cyber security risk management
Commonly, cyber security is evaluated under the umbrella of overall company enterprise risk. Executives and board members want to understand and monitor their organization's risk exposure from a cyber security perspective, but often lack appreciation for how complex developing and implementing an effective cyber security architecture can be.

Improving cyber security posture
Most organizations collect massive data, but are not equipped to use it effectively. With an understanding of the risks and priorities facing their organizations, executives can make data-driven decisions about cyber security investments.

Cyber Security Risk Assessment
The starting point to better cyber security

Addressing cyber security risk is a journey

Your goal is to improve the risk profile of your systems year over year. Remediating risks can be costly and time consuming. The results of a risk assessment help strike a balance between addressing the highest risk gaps while being mindful of the financial and personnel resources available.

ABB Cyber Security Risk Assessment supports plant operations and enterprise risk managers to understand, monitor and address their control system cyber security risk. A risk assessment is necessary to identify and prioritize the cyber security risk relevant to the specific control system under evaluation. Only with this visibility can operators have assurance that they are taking strategic steps to improve their security posture.

The risk assessment is performed by ABB experts with deep domain expertise in both ABB control systems and cyber security. This combination of skill sets can be vital to assessing risk of an industrial operation.

—

How can ABB help you achieve your goals?

- Understand risk and act accordingly
- Address highest impact activities
- Align to regulatory requirements
- Develop a remediation plan to rectify risks
- Demonstrate progress year over year
- Maintain a cost-effective, robust security posture

1 Basic Risk Assessment

ABB will evaluate the system under consideration to determine and assess system risks. The output is a report that highlights the risks identified, prioritizes those risks and provides remediation steps, down to the zone and conduit level.

How does it work?

An ABB cyber security expert will:

- Prepare and gather inputs, including the collection of items like network diagrams, information on recent cyber security incidents and asset inventory
- Determine scope to define the system under consideration
- Conduct an on-site workshop after reviewof collected documentation
- Partition the system under consideration into zones and conduits
- Document the results in a report
- Provide a risk rating based on criticality, likelihood and consequences

2 Detailed Risk Assessment

A detailed risk assessment builds on the basic risk assessment and is conducted for each zone and conduit. Typically, it is requested if a specific zone or conduit demonstrates risk levels above the desired threshold.

In most cases, zones and conduits have common cyber security requirements based on factors such as criticality or likelihood. Therefore, cyber security practices and requirements can be applied similarly throughout.

Greater visibility for better risk management

Make lasting improvements faster

Time and money savings

International standards call for a cyber security risk assessment annually to demonstrate an improved security posture year over year.

- ABB Cyber Security Risk Assessment reduces the time and money spent performing these assessments. With ABB's deep domain expertise and proven track record allows your organization to invest those savings into other endeavors to grow business.

Improved control system risk management

Risk is traditionally presented to company boards and executives collectively. Boards are evaluated on measuring risk and are personally liable for their decisions. But understanding the steps to mitigate and contain risk within an organization can be daunting.

- By working with ABB, these identified risks will be aligned to your enterprise risk management process and risk tolerance levels.

Access to cyber security experts

ABB cyber security experts have a clear understanding of control system vulnerabilities and are diligent in monitoring current and future areas of concern.

- With ABB, you gain access to a dedicated group of experts that is constantly monitoring cyber security vulnerabilities and malicious activity.

Downtime avoidance

Cyber security risks can have substantial impact on productivity. In the worst case scenario, your operation could fall victim to a cyber attack, halting production completely until a solution can be implemented. Even in the best case scenario, your in-house technicians are likely IT professionals who lack the control system expertise to optimize cyber security updates to avoid downtime.

- Working with ABB experts specializing in control system cyber security to identify and implement these improvements will help your organization avoid unplanned downtime and minimize any planned downtime required.

How much is your cyber security worth?

Plan ahead with a detailed risk assessment

Tap into ABB Cyber Security experts on demand

Instead of having a dedicated in-house team, leverage trained experts both on your control system and the application of cyber security controls to that system.

- Ensure the quality of the assessor
- Reduce time and costs
- Stay on top of cyber threats

$150K+ for a typical resource

3 years of experience per resource

Align directly to the standard

Reduce time by relying on experts that work closely with regulatory standard boards and work groups. Your assessment will be aligned to the latest international regulations.

- Avoid fines
- Reduce training time and costs on developing in-house processes and procedures

$100K+ time spent developing in-house processes and procedures

Potential millions in fines avoided

Take high-impact actions cost effectively

With ABB, understand how to prioritize your security efforts. Easily gauge your progress with a visual representation of improvements.

- Leverage data
- Plan for future investments
- Demonstrate commitment to cyber security

340 hours for data consolidation

60 hours for budget planning

Let's talk

How are you staying aware of your future cyber security risks?

When was the last time you did a cyber security risk assessment?

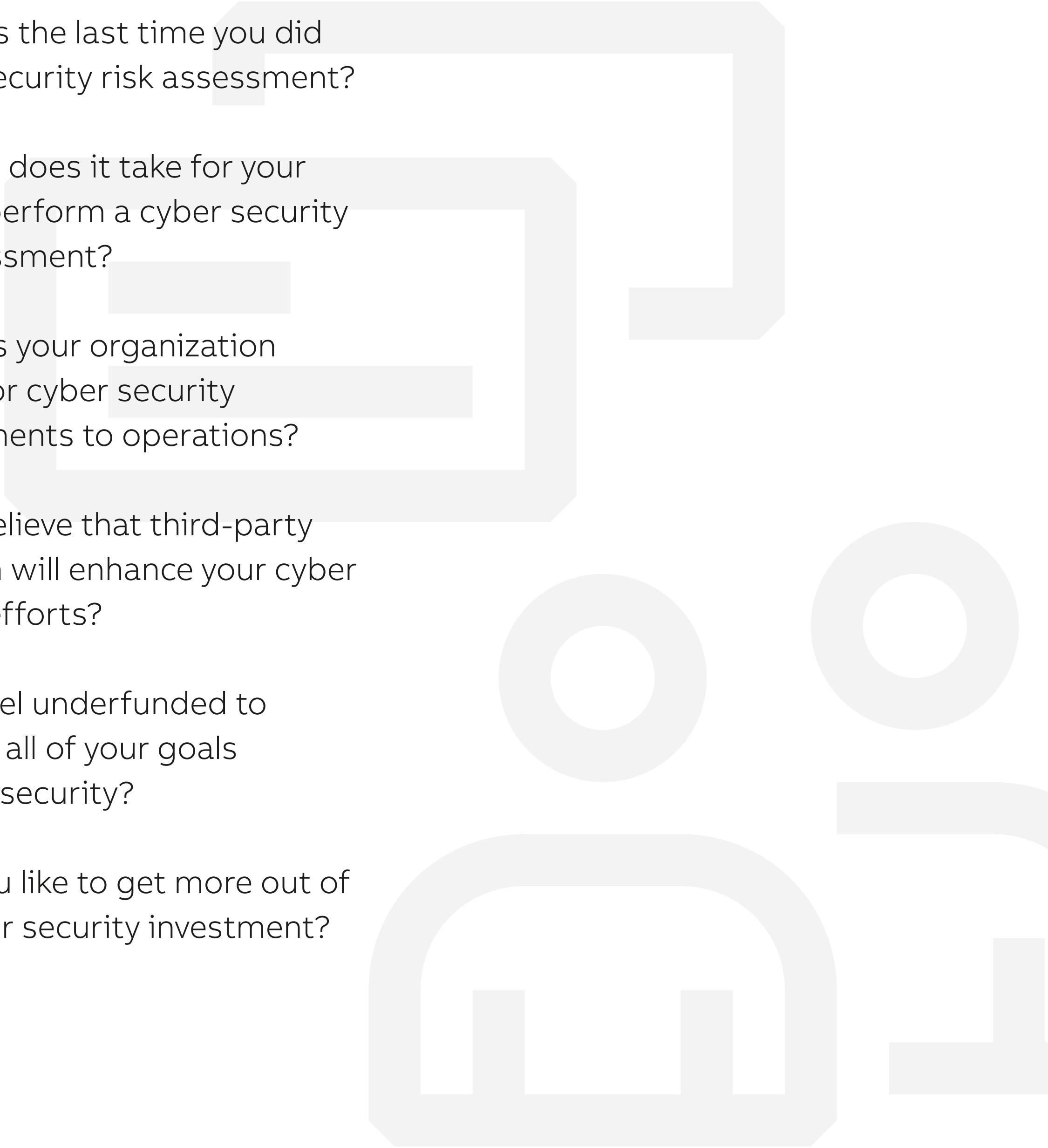
How long does it take for your team to perform a cyber security risk assessment?

How does your organization budget for cyber security improvements to operations?

Do you believe that third-party validation will enhance your cyber security efforts?

Do you feel underfunded to complete all of your goals for cyber security?

Would you like to get more out of your cyber security investment?



—

ABB Ltd.
Operating in more than 100 countries.
Energy Industries
Industrial Automation

campaign.abb.com/risk-assessment