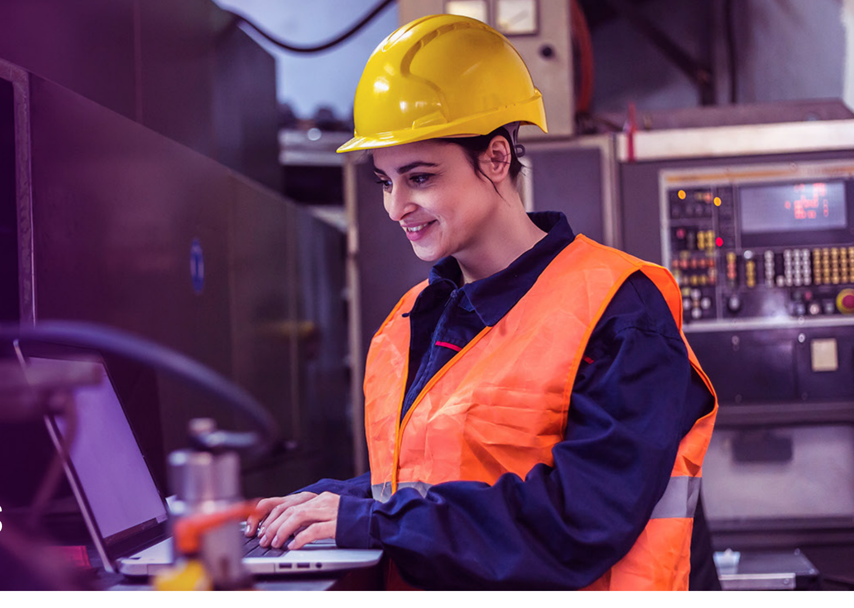
AVEVA

Industrial cybersecurity: Protecting your digital transformation initiatives



The industrial landscape has never been more uncertain, or more ready for digital transformation. With the need to enable remote work and team collaboration, technologies such as Cloud, Edge and IIoT not only provide new ways to enhance business performance, but also pave the way for improved business processes and procedures. Along with safety, the most critical area to address during this change is industrial cybersecurity.

Cybersecurity by the numbers

+2100%	5,200	279 days	$3.92 million	$133.7 billion
Increase in industrial cyber attacks over the past three years	The average number of attacks on IoT devices per month	Average time to identify and contain a data breach	Typical financial impact of a single cyber attack. Source: IBM Security	Forecasted spend on cybersecurity by 2022 Source: Gartner

Rapid advances in technology have seen a corresponding rise in cybersecurity risks. Yet according to most experts, industrial systems are not protected well enough. With many underestimating the risks and impact a breach may have on their business.

Cybersecurity requires a proactive stance involving the entire organization. Balance needs to be achieved between mitigating risks and enabling new business initiatives. Focus not only on training staff but on selecting appropriate technology partners.

The safety and security of your data is our top priority.
As an established leader with over 50 years experience delivering industrial software portfolio, we recognize that your data demands a stringent cybersecurity posture and the highest set of operating standards.

The proof is in the portfolio

Deployed in **100,000+** sites globally

Processing **10+ Trillion** industrial transactions per day

Monitoring **20 Billion** industrial parameters

Storing and managing **12,000 TB** of information per year

Key security considerations for operational technology

End-to-end security

Connected devices
We build security from the ground up – using components that meet recognized standards, and include enforced encryption.

Edge control
We incorporate security protection into our system design and development process, including rigorous testing and validation.

Apps, analytics, and cloud services
Security must be integral to design and fundamentally built into the services that support the operation of your systems.

Potential risks of an OT breach

- Extreme cases could result in loss of life
- Exposure of intellectual property
- Lost production and waste
- Serious environmental impact
- Serious fines and penalties
- Damaging brand and reputation loss

Your cybersecurity checklist

Cybersecurity is a multi-faceted discipline requiring a proactive approach across the business. Best-prepared businesses report a focus on the following key areas.

People
- Invest in security training for staff, contractors and 3rd parties
- Educate on dangers of USBs, malware, phishing
- Make your people active cybersecurity partners

Network
- Ensure a unidirectional gateway between IT and OT systems
- Run vulnerability scans and issue patches regularly
- Install anti-malware solutions for industrial end points

Partners
- Select vendors that will partner with you to protect your critical data
- Understand their security, privacy and legal policies
- Determine where your data will be collected and stored

Processes
- Develop, document and validate your cybersecurity program
- Ensure cross department buy-in e.g. from management, IT, security
- Cover a range of activities including security audits and vulnerability scans

Devices
- Change your IoT device passwords from the factory default
- Extend your security and password policies to mobile devices
- Conduct regular intrusion testing and anomaly detection on your devices

Cybersecurity checklist for your vendor

When it comes to cybersecurity, who you partner with is crucial. Software vendors play an important part in your cyber defence strategy. When considering a cloud or IIoT partner here are some key questions to consider.

Physical security
- Where are their cloud services physically deployed?
- Where will my data actually reside?
- Where and how will my data be captured, stored and used?

Data security
- How is your information protected – at rest and in motion?
- Does your vendor support unidirectional data transfer?
- How does your supplier deal with network outages?

Application security
- How do they handle authentication, authorization and account management?
- What is their approach to identity and access management (IAM)?
- Do they offer a flexible, scalable solution?

Continuous monitoring
- Do they have proactive monitoring and active security policies in place?
- Can they identify abnormal behavior and catch anomalous activity?
- What procedures are there to detect and isolate suspicious activity online?

Security assessments
- Do they have a proactive program of external security audits?
- How do they deal with ongoing compliance with regulations e.g. GDPR?
- Do they have a published security statement that you can read?

Projects and delivery
- Are their project delivery teams certified to global standards such as CMMi Level 5, or ISO 9001?
- Do they have a Computer Security Incident Response Team (CSIRT) ready to mobilize?
- Do they have strategic partnerships with key security experts such as Cylance or Claroty?

We are dedicated to earning and retaining your digital trust. That is why we transparently publish our security statement. View it for yourself at trust.aveva.com

Counted on by the world's most trusted industrial leaders

550+	4,600	9/10	3,200+	1,000+
Refineries	Food and beverage processing plants	Shipyards	Infrastructure customers	Power generation units

There is no better time to take advantage of the IIoT and cloud technologies. Digital transformation is a journey that allows you to transform your existing automation investment into an improved way of doing business.

Speak to an expert

AVEVA

www.aveva.com | linkedin.com/company/aveva | @avevagroup | facebook.com/avevasolutions