

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%

Increase in industrial cyber attacks over the past three years

5,200

The average number of attacks on IoT devices per month

Rapid advances in technology have seen a corresponding

279 days

Average time to identify and contain a data breach

\$3.92 million Typical financial impact

of a single cyber attack. Source: IBM Security

\$133.7 billion Forecasted spend on cybersecurity by 2022 Source: Gartner

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.

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.

Cybersecurity requires a proactive stance involving

## As an established leader with over 50 years experience delivering

The safety and security of your data is our top priority.

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



100,000+ sites globally

Monitoring

Deployed in

10+ Trillion industrial transactions per day



20 Billion industrial parameters

of information per year Key security considerations for operational technology

Storing and managing

12,000 TB





ground up – using components that meet recognized standards,

and include enforced encryption.

We build security from the

We incorporate security protection into our system design and development process, including

rigorous testing and validation. Potential risks of an OT breach

and cloud services Security must be integral to design and fundamentally built

into the services that support the operation of your systems.



in loss of life



of intellectual property





impact





### Cybersecurity is a multi-faceted discipline requiring a proactive approach across the business.

Your cybersecurity checklist

People

Best-prepared businesses report a focus on the following key areas.



### Educate on dangers of USBs, malware, phishing

 Make your people active cybersecurity partners

Invest in security training for staff,

contractors and 3rd parties

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

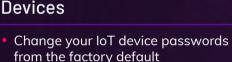
be collected and stored

Cybersecurity checklist for your vendor When it comes to cybersecurity, who you partner with is crucial. Software vendors

### Develop, document and validate your cybersecurity program

**Processes** 





Ensure cross department buy-in e.g.

from management, IT, security





## anomaly detection on your devices

### 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?

 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?

play an important part in your cyber defence strategy. When considering a cloud or IIoT partner here are some key questions to consider.

Data security



## 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?
- Security assessments Do they have a proactive program of external security audits?



550+

Refineries

Projects and delivery • Are their project delivery teams certified to global standards such as CMMi Level 5, or ISO 9001?

• Do they have a published security statement that you can read?

How do they deal with ongoing compliance with regulations e.g. GDPR?

Can they identify abnormal behavior and catch anomalous activity?

What procedures are there to detect and isolate suspicious activity online?

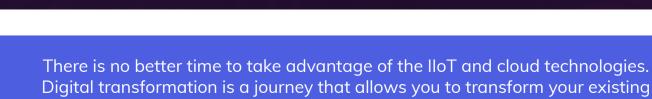
We are dedicated to earning and retaining your digital trust. That is why we transparently publish our security statement. View it for yourself at trust.aveva.com

Counted on by the world's most trusted industrial leaders

9/10

Shipyards

 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?



Speak to an expert

automation investment into an improved way of doing business.





3,200+

Infrastructure

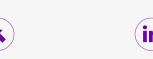
customers



1,000+

Power generation

units



AVEVA and the AVEVA logo are a trademark or registered trademark of AVEVA Group plc in the U.S. and other countries.

www.aveva.com

© 2020 AVEVA Group plc and its subsidiaries. All rights reserved.

4,600

Food and beverage

processing plants