Cybersecurity checklist for your vendor

When selecting a vendor, don’t just look at their products. Members play an important part in your cybersecurity strategy. When implementing a new technology, it’s essential to ensure proper governance and identify the right partners.

Check out our cybersecurity checklist for your vendor and ask the following questions:

1. **Physical security** - How secure is their data center? Does their location support your SLAs?
2. **Data security** - What measures do you have in place to protect the data? How will you encrypt sensitive data?
3. **Application security** - Are there any known vulnerabilities in your products? How are they being addressed?
4. **Continuous monitoring** - Who will be responsible for monitoring the network? Are there any tools in place to detect and respond to threats?
5. **Security assessments** - Are there any security frameworks or standards that they adhere to?

The safety and security of your data is our top priority. At AVEVA, we have experienced professionals who are dedicated to earning and retaining your digital trust. That is why we transparently incorporate security into our entire workflow process, including rigorous testing and validation. Cybersecurity requires a proactive stance involving every aspect of the business, from management, IT, and security to cross-functional teams.

Cybersecurity by the numbers

- **9/10** of organizations report costs associated with data breaches
- **$133.7 billion** Forecasted spend on cloud services by 2024
- **279 days** Average time to identify and contain a data breach
- **$520 million** Average fine in a data breach
- **$225 billion** Global spending on cybersecurity services by 2025
- **$1.3 trillion** Global spending on cybersecurity services by 2025

**Key security considerations for operational technology**

- **End-to-end security** - Ensure a unidirectional gateway is in place to protect your systems.
- **People** - Make your people active cybersecurity partners.
- **Processes** - Ensure cross-departmental buy-in to your cybersecurity plan.
- **Partners** - Identify and contain any abnormal behavior.
- **Compliance and data privacy** - Ensure your processes comply with regulations like GDPR.
- **Threat intelligence** - Understand their security, privacy, and development process, including rigorous testing and validation.

**Potential risks of an OT breach**

- **60%** of attacks on IoT and IIoT devices per month
- **$12,000 TB** Storing and managing intellectual property
- **20 billion+** Monitoring devices per year
- **4,600** Typical financial impact of a single cyber attack
- **279 days** on average to identify and contain a data breach
- **9/10** of organizations report costs associated with data breaches

**2021 cybersecurity report**

The COVID-19 pandemic has accelerated digitalization across industries. As a result, cybersecurity has become even more critical. In 2020, AVEVA experienced a 12% YoY increase in industrial cybersecurity vulnerabilities. As enterprises continue to embrace cloud-based technologies, cybersecurity is more important than ever.

**Where will your data actually reside?**

- **3,200+** Devices per month
- **279 days** Time to identify and contain a data breach
- **$12,000 TB** Storing and managing intellectual property
- **20 billion+** Monitoring devices per year
- **4,600** Typical financial impact of a single cyber attack
- **9/10** of organizations report costs associated with data breaches

Cybersecurity is a multi-faceted discipline requiring a proactive approach across the business. We incorporate security into our entire workflow process, including rigorous testing and validation. Cybersecurity requires a proactive stance involving every aspect of the business, from management, IT, and security to cross-functional teams.

**Your cybersecurity checklist**

- **Physical security** - Ensure your data center is secure. How can you ensure your security policy is followed?
- **Data security** - What measures do you have in place to protect the data? How will you encrypt sensitive data?
- **Application security** - Are there any known vulnerabilities in your products? How are they being addressed?
- **People** - Make your people active cybersecurity partners.
- **Processes** - Ensure cross-departmental buy-in to your cybersecurity plan.
- **Partners** - Identify and contain any abnormal behavior.
- **Compliance and data privacy** - Ensure your processes comply with regulations like GDPR.
- **Threat intelligence** - Understand their security, privacy, and development process, including rigorous testing and validation.

Cybersecurity requires a proactive stance involving every aspect of the business, from management, IT, and security to cross-functional teams. By implementing a robust cybersecurity strategy, you can protect your digital assets and ensure business continuity.

To learn more and download our cybersecurity report, visit our dedicated page on the AVEVA website.