

Cyber Risk Insurance Partners

Reduce the financial impact of security incidents

Digital transformation means that industrial networks are becoming more connected and more productive - but also more exposed.

When an industrial company suffers a cyber or ransomware attack, there is a lot more at stake than data. Cyberattacks on industrial locations can cause property damage, injure people or interrupt operations. Research firm Gartner predicts that the financial impact of attacks on industrial systems resulting in fatal casualties will reach over \$50 billion by 2023. Even without adding the incalculable value of a human life into the equation, the costs for organizations in terms of compensation, litigation, insurance and reputational damage is enormous.

An attack on industrial networks typically coincides, or is preceded by, a breach of the IT or enterprise network. This means that regulatory fines concerning data privacy are another aspect to be considered. The General Data Protection Regulation (GDPR) that came into effect in 2018 introduced strict reporting obligations with regard to cyber incidents – which need to be reported within 72 hours. Cyber breaches today lead to significantly greater sanctions, including administrative fines of up to 4% of global revenue or €20 million.

OTORIO delivers a full suite of industrial cybersecurity services. Our staff brings years of experience forged in elite military cyber forces. Serving some of the world's leading manufacturers, OTORIO enables organizations to defend against and quickly recover from cyberattacks – safeguarding reliable, resilient and efficient production.

- Commence investigation of cyberattacks within hours
- Leverage existing security products to speed up mitigation processes
- Work closely and seamlessly with IT and operational teams
- Conduct deep and fast root cause analysis to spot patient zero and uncover attack vectors
- Achieve speedy recovery to bring operational networks back online
- Resolve cyberattacks from remote to save travel time and avoid travel restrictions

financial impact of
attacks on industrial
systems

**over \$50 billion
by 2023.**

Gartner

OTORIO's Services Suite

	ASSESS	PREVENT	DETECT	RESPOND	RECOVER
Incident Response				V	V
Industrial Cyber Risk Assessment	V	V			
Industrial Penetration Testing	V	V			
Cyber Threat Intelligence	V				
Managed Detection and Response			V	V	V

OTORIO's 24/7/365 Service Coverage



Assess

Comprehensive risk assessment to detect exposed and leaked data including assets, email addresses, passwords, intellectual property and more.

Detect

When an incident is detected in its early stage, it is quicker to resolve and causes less damage. OTORIO's experienced OT cyber analysts work together with organizational IT security teams to detect and mitigate incidents before any damage can be done.

Prevent

Apply threat analysis and specified red-team penetration test methodologies to detect vulnerabilities and seal them.

Respond

A seasoned incident response team, available 24/7/365, brings years of hands-on experience forged in elite military cyber forces.

Recover

Restoring entire networks within hours to allow organizations to quickly recover from malware and ransomware attacks and resume full productivity.

Why Insurers Need an OT Cybersecurity Partner

IT cybersecurity experts are crucial for any business. Yet IT cybersecurity specializes in securing bits and bytes alone, whereas OT cybersecurity is experienced in securing both data and physical systems.

It's a unique specialization, especially because OT components often communicate via industry-exclusive protocols, that are not even visible to IT networks.

Given OT cybersecurity's focus on physical systems, OT teams are trained to prioritize safety first – as opposed to IT, who tend to first focus on confidentiality over other considerations. OT cybersecurity experts are experienced in dealing with physical systems that require stable values and meticulous control. After all, when things go awry in an OT network, direct physical harm and production stoppage are the main concerns.

Suspect a Breach? Incident Response Hotline



+43 720 775263



response@otorio.com

About OTORIO

OTORIO combines the experience of top nation-state cybersecurity experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. Our comprehensive portfolio of services empowers industrial companies to implement, automate, and operate secure production, making way for a safer, more reliable and productive industry. Industrial Cybersecurity Plus cyber experts work closely with cyber and operational teams to tailor solutions that address your specific industrial digital security needs.