Addressing industrial cybersecurity risks affecting the industry

OTORIO & ANDRITZ partner to safeguard production operations
Daniel Bren, Co-Founder and CEO, OTORIO

INTRODUCTION:

The pulp and paper industry continues its rapid digital transformation. This makes pulp and paper manufacturers' industrial networks more connected, more productive — and, unfortunately, more exposed to cybersecurity risks. Safeguarding IT and operational technologies (OT) is critical to ensuring business continuity and resilient operations at the heart of pulp and paper manufacturing.

As industry leader ANDRITZ's OT cybersecurity partner, OTORIO knows how crucial safety, uninterrupted energy supplies, plant operations, and reliable utilities are to the pulp and paper manufacturing processes. The sophisticated industrial machines crafted by ANDRITZ rely on multiple technologies, data sources, automation, and digitalization, as well as procedures to optimize process performance.

Manufacturers worldwide have been hit with real-world industrial cybersecurity attacks that halt industrial operations, lead to ransomware demands, harm business continuity, and affect shareholder value. The pulp and paper industry is no exception. Over the past two years, cyber attacks impacted the manufacturing operations of at least three different paper and packaging companies in North America and Europe.

Whether they deal with recycling OCC, packaging board, and mixed waste, securing production lines, drying processes, or power and boiler generation, OTORIO's industrial-native cybersecurity solutions enable pulp and paper manufacturers to minimize digital and cyber risks to their industrial operations. Our solutions prioritize risk mitigation, add business context, and allow plants to manage multi-site OT, IT, and IIoT networked environments from one central dashboard.

Why the industry faces cybersecurity vulnerabilities

Whether producing paper, boards, or tissue, the various stages of pulp and paper production and the technologies that support it increase a manufacturer's digital attack surface. Producing panelboard, for example, involves heavy industrial machinery and automated, networked technologies for raw wood processing, preparation, cleaning, and pressurized refining. If a cyber attack impacts even one stage of the process, this can have a domino effect on related processes, potentially disrupting or halting operations until the security breach is resolved.

OTORIO is proud to fully integrate our OT cybersecurity solutions into ANDRITZ's safe automation and digitalization smart manufacturing portfolio. Our solutions enable a pulp and paper manufacturer's OT and IT teams to proactively reduce cyber risks and vulnerabilities affecting the security and safety of manufacturing procedures, business continuity, and ongoing operations. We provide plants and production floors with key functions like enhanced visibility of all your digital assets across your manufacturing network (whatever their location). Your teams get contextualized risk management with easy-to-use mitigation playbooks and significantly more resilient industrial operations.

Critical infrastructure

It is also imperative for pulp and paper manufacturers to protect their internal critical infrastructure assets in their mills and plants from cyber threats and vulnerabilities. Many stages of production and processing create opportunities to recover, conserve, and reuse resources that might otherwise go to waste (e.g., wood fiber, water, and energy). Water is essential to the pulp and paper manufacturing process. Manufacturers use it in many stages of production: wood preparation, pulping, pulp washing, bleaching, and coating. Recovery boilers allow for the extraction, recovery, and reuse of byproducts like black liquor as energy during other stages of production. For example, boiler generators serve two functions: supplying steam for paper production and generating power for manufacturing operations.

"ANDRITZ's pulp and paper industry clients benefit from OTORIO's industrial-native OT cybersecurity solutions. By proactively reducing digital risks and vulnerabilities in their multi-step manufacturing processes, they help maintain secure, resilient operations for our clients' paper, board, and tissue production."

- Tatu Liimatainen, Head of OT Cybersecurity, ANDRITZ

ANDRITZ's steam recovery systems enable the efficient capture and reuse of surplus steam energy, reducing a manufacturing plant's fuel and boiler feed water consumption. Industrial burner solutions also supply pulp and paper mills with energy by repurposing industrial waste and biofuels to generate energy and reduce CO2 emissions. Industrial machinery in pulp and paper plants that support energy production, capture, or reuse can also affect worker safety if malicious actors breach OT or IT systems controlling their operation.

Safeguarding and having visibility into your IT and OT assets is vital. Without effective OT security, malicious cyber actors are more likely to breach security configurations in industrial assets like boiler generators, steam recovery systems, and fuel systems. Such breaches can impact worker safety, day-to-day operations, regulatory compliance, and more.

Preventing cyber risks from third parties

Your pulp and paper business uses third-party software solutions and works with contractors who might be a source of accidental or malicious cyber incidents. Contractors help service your heavy machinery, integrate new equipment and processes, and interface with power, utility, and energy systems on which your organization depends.

Contractors are often unaware of cyber risks and can introduce vulnerability into your networks. An effective OT security risk management solution will identify such threats and help you implement safety practices to prevent them from being exploited.

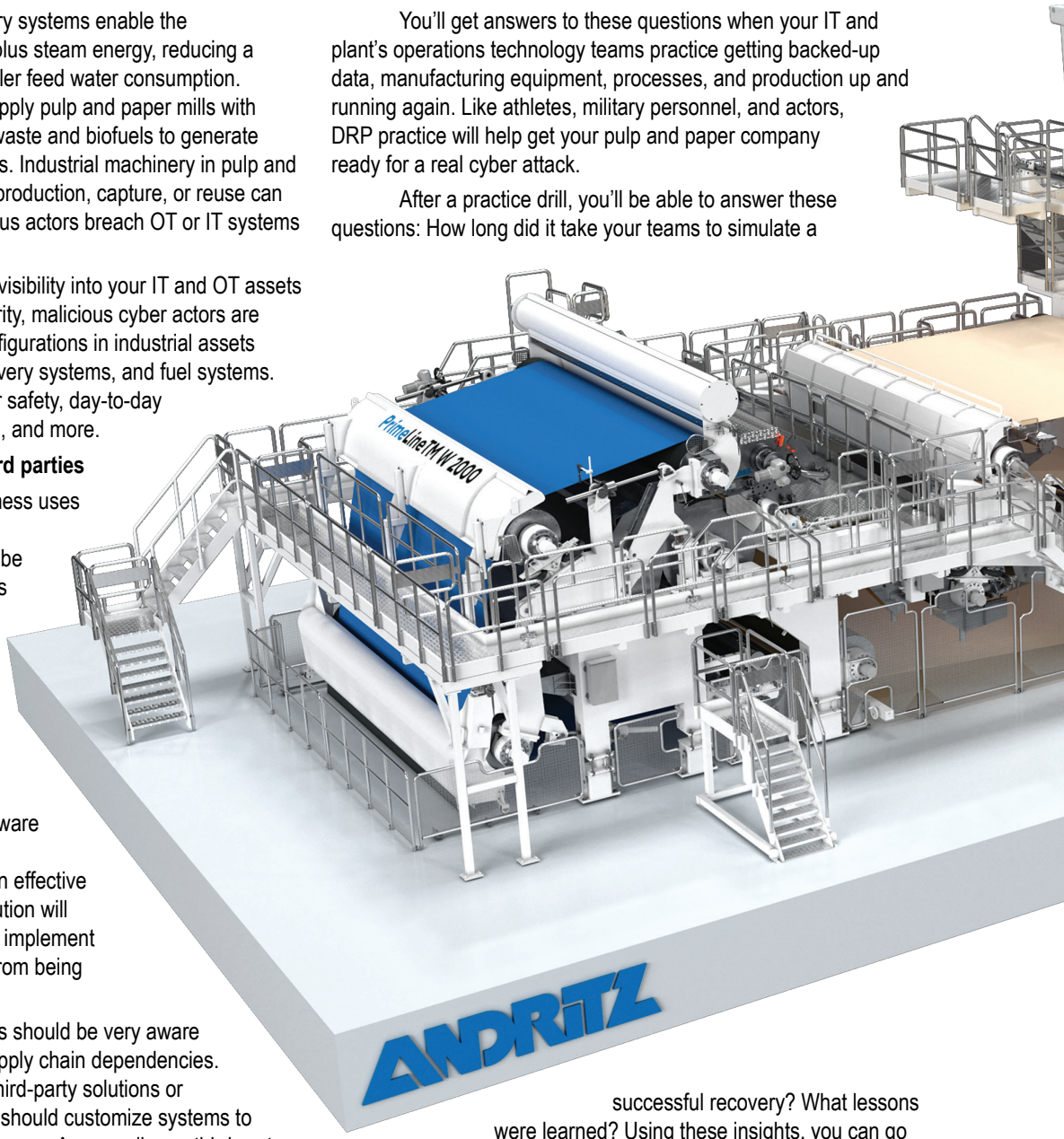
Pulp and paper companies should be very aware of potential risks introduced by supply chain dependencies. In cases where products rely on third-party solutions or services to operate, the company should customize systems to minimize their use and risk of exposure. Assess all your third-party products and providers associated with your business operations with a comprehensive due diligence program.

Practice makes perfect: Disaster recovery exercises

Every pulp and paper manufacturer needs to have a disaster recovery plan (DRP) and a backup plan in place. The most effective way to recover from an industrial cyber attack is to practice your DRP and backup plans often.

You'll get answers to these questions when your IT and plant's operations technology teams practice getting backed-up data, manufacturing equipment, processes, and production up and running again. Like athletes, military personnel, and actors, DRP practice will help get your pulp and paper company ready for a real cyber attack.

After a practice drill, you'll be able to answer these questions: How long did it take your teams to simulate a successful recovery? What lessons were learned? Using these insights, you can go back and repeat your DRP.

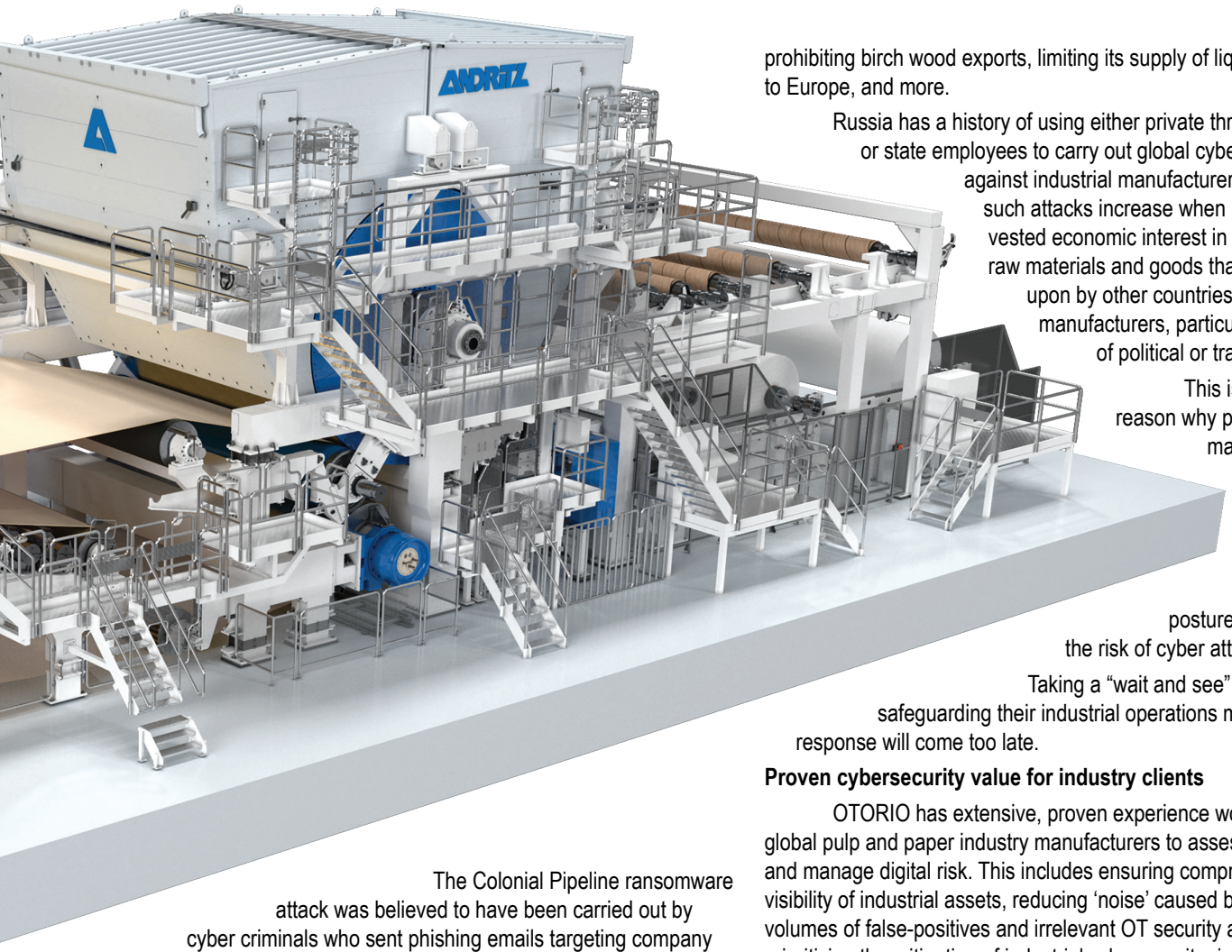


Why employee cyber hygiene is important

It is imperative that every pulp and paper company require its employees to practice basic cyber hygiene. At a minimum, this means workers should a) use multi-factor authentication (MFA) for remote access to the company's network, b) control user-access management, and c) use reliable anti-virus and firewall solutions.

Hackers frequently try to gain access to a company's IT and OT networks via -'phishing'- campaigns that target employees' corporate email and social media accounts. These attack strategies often ask employees to 'confirm' their account login details, including their passwords. If an employee shares such secure credentials, this may give malicious actors access to the employee's account and provide remote access to the company's internal network, databases, industrial operations, and machinery.

- ***Do your IT and OT teams regularly back up network data and secure these backups?***
- ***Do you know how often backups are done and where your data is stored (e.g., locally, offsite, or in multiple locations)?***
- ***Does your company hold regularly-scheduled disaster recovery exercises every quarter?***
- ***When a zero-hour or zero-day attack happens, will your DRP actually work?***



The Colonial Pipeline ransomware attack was believed to have been carried out by cyber criminals who sent phishing emails targeting company employees. Employees who shared their credentials reportedly allowed hackers to exploit remotely accessible accounts, systems, and more.

That is why employee cyber awareness training is essential. Pulp and paper manufacturers should train all employees in security awareness subjects related to their role and develop a security awareness training plan. Topics on which to educate employees during this training include the company's information security policy, IT and OT access, best practices, and access to relevant machines and systems by authorized users only.

Financially-motivated ransomware attacks

Many cyber attacks can result in ransomware demands. Pulp and paper manufacturing is a multi-billion dollar global industry. The recent pandemic increased demand for corrugated cardboard and pulp production. From toilet paper and package shipments to paper goods for food deliveries, CIPA (the European association representing the paper industry) noted this trend in its 2021 annual statistics.

Criminal ransomware gangs try to find and exploit any OT and IT security vulnerabilities that industrial manufacturers have. We know of at least three real-world cyber attacks against pulp and paper manufacturers. Two of these attacks in North America resulted in ransomware demands.

Geopolitical risks impact manufacturing operations security

Like other industries, geopolitical conflicts can increase OT and IT security risks for pulp and paper manufacturers. After Russia invaded Ukraine, sanctions imposed on Russia by the US and EU affected supply chain security for raw materials like Russian birch trees. Until recently, these trees' pulp was relied on to soften toilet paper tissue. Russia responded to these sanctions, in part, by prohibiting birch wood exports, limiting its supply of liquid natural gas to Europe, and more.

Russia has a history of using either private threat actors or state employees to carry out global cyber attacks against industrial manufacturers. The risks of such attacks increase when Russia has a vested economic interest in trading its own raw materials and goods that are relied upon by other countries and foreign manufacturers, particularly in cases of political or trade disputes.

This is an important reason why pulp and paper manufacturers should proactively enhance their IT and OT security postures to reduce the risk of cyber attacks.

Taking a "wait and see" approach to safeguarding their industrial operations means any response will come too late.

Proven cybersecurity value for industry clients

OTORIO has extensive, proven experience working with global pulp and paper industry manufacturers to assess, monitor, and manage digital risk. This includes ensuring comprehensive visibility of industrial assets, reducing 'noise' caused by high volumes of false-positives and irrelevant OT security alerts, prioritizing the mitigation of industrial cybersecurity risks based on their context and potential impact on your business.

We have experience reducing ransomware risks and helping companies fight phishing attempts that target thousands of employees at hundreds of worldwide locations. Our work leads to improving customers' security controls to ensure their OT, IT, and IIoT network environments are resilient against future attacks.

OTORIO has deep experience performing vulnerability and penetration testing ('pen testing') for pulp and paper manufacturers. This allows you to see how outside attackers would view your company's IT and operational technology (OT) networks. These valuable tests and analyses enable us to find potential attack scenarios and help you proactively reduce vulnerabilities. We have years of experience helping industry manufacturers prioritize and contextualize risks that can have the greatest impact on their businesses.

OTORIO and ANDRITZ help safeguard your operations

ANDRITZ helps its global pulp and paper customers minimize digital and cyber risks through its partnership with industry-leading OT security provider OTORIO. Founded by leading OT cybersecurity experts, OTORIO's portfolio of industrial-native cybersecurity solutions ensures continuous digital risk management and compliance. These solutions are now fully integrated into the ANDRITZ Automation & Digitalization portfolio, providing customers with safer machines and a significantly more resilient infrastructure

In a multi-generational, constantly changing threat environment, customized OT cybersecurity measures are an imperative part of the automation development process. That is why ANDRITZ embeds OTORIO's innovative solutions in its market-leading solutions and services, ensuring that every pulp and paper machine meets the highest cybersecurity standards.

The advanced services are delivered in the safest way, ensuring the customer's continuous efficient and effective production, along with proprietary commercial data security.

In today's rapidly evolving industrial operations environment, protection against cybersecurity risks and compliance with industrial security standards is expected upon every machine delivery and commissioning. ANDRITZ ensures that each machine it delivers is secure, regulatory compliant, and meets the customer's contractual requirements for continuous, safe production.

With OTORIO's spOT Lifecycle solution, ANDRITZ can also also provide post-delivery Security-as-a-Service over the machine's entire lifecycle on the customer's premises. spOT Lifecycle periodically checks configurations and vulnerabilities during ANDRITZ service calls (whether remotely or on-site), and performs "virtual querying" of the machine's fingerprint for new, publicly-known vulnerabilities. This solution provides clear, practical recommendations on how to remediate compliance and security gaps and harden against ransomware attacks.

The result is a detailed report on compliance confirmation that delivers accurate, in-depth security verifications of the delivered machines. spOT Lifecycle enables ANDRITZ to remediate each vulnerability, security gap, and compliance deviation prior to a machine's delivery, and include details on any mitigation steps taken in the issued report. The information is also used to ensure that new deliveries are secure by design.

ANDRITZ's Automation & Digitalization embeds OTORIO cybersecurity into the automation lifecycle of new and existing machines for safe, resilient, and efficient operations. The company's Security-as-a-Service offering ensures that each machine it delivers is secure, regulatory compliant, and meets contractual requirements. Every customer is assured that ANDRITZ deliveries provide continuous, safe production throughout their entire lifecycle.

Real-world cyber attacks on industry manufacturers

In February 2021, Atlanta-based corrugated packing manufacturer WestRock experienced a ransomware attack. A month later, the company informed shareholders that the attack had affected WestRock's production operations, causing a loss of approximately 125,000 tons in containerboard and paperboard production.

In February 2020, a malware attack on Paper Excellence Canada impacted the company's IT systems and forced it to temporarily shut down operations at three of its nine production facilities. Hackers installed malware on the pulp and paper manufacturer's IT system software that sent essential data to production mills, telling manufacturing operations machines about required criteria like paper quantities and dimensions. The manufacturer's Canadian operations had to be temporarily halted until the attack could be resolved.

In January 2022, the Swiss-based CPH group experienced a cyber attack on its IT systems that caused it to temporarily suspend pulp and paper manufacturing operations at plants in Perlen, Switzerland and Mülheim, Germany. Approximately two weeks after the attack, the company announced that "all IT systems of the CPH Group worldwide were checked and restored from the backup systems together with external cyber specialists."

For secure remote access to operational assets, ANDRITZ Automation & Digitalization utilizes OTORIO's remOT to deliver secure, simple, and fully governed remote access to the operational environment.

ANDRITZ applies remOT zero trust security architecture as a service in clients' industrial environments in compliance with IEC standards for single sign-on controlled access to operational assets. Alternatively, clients can easily manage remote connections for all their third-party vendors by using remOT.

Summary

Industrial cybersecurity risks and ransomware demands affecting pulp and paper manufacturers' production are an unfortunate reality. Companies must proactively assess, manage, and mitigate OT security risks to protect business continuity and maintain resilient operations.

OTORIO and ANDRITZ bring their extensive experience and industrial-native cybersecurity expertise to help you assess, monitor, and manage industrial risks. From helping to ensure safe pulp and paper manufacturing operations to reducing risks and vulnerabilities that can impact your production, worker safety, critical infrastructure, and regulatory compliance, our proven OT security solutions and services can enhance your cybersecurity posture and help safeguard your industrial production.

Daniel Bren, Co-Founder and CEO, OTORIO