Protecting Pulp and Paper Mills from Ransomware Attacks

The most powerful tool any engineer can possess in this modern connected landscape is data. Ones and zeros are the foundation for just about everything in modern Industry 4.0 driven operations, including pulp and paper. As a result, digital transformation — underpinned by smart technology — has become the most important operational exercise any business can perform.

Modern paper, board and packaging mills are dependent on sophisticated computer-controlled automation systems and this smart technology is all about delivering agility, flexibility, and efficiency. However, with one eye on recent headlines, it is equally important to also consider security, especially if you rely on legacy technology, which does not have any form of embedded security.

From an infrastructure perspective, to be fully digitally transformed, you must be fully connected. And when you’re fully connected you introduce what the IT industry likes to call threat vectors — potentially open routes/gateways — into your system. With a major part of digitalization being the convergence of operational technology (OT) with IT systems, these gateways can open up a much larger mixed digital ‘playground’ for hackers than they would have done a few years back.

These days, companies who weren’t traditional targets of cyberattacks are making headlines more and more because any industry that is sensitive to downtime is an ideal target for money-making criminals. To make sure you have the proper protocols in place, you need to understand why and where manufacturing is becoming more
vulnerable, what the standards are and how that translates to pulp and paper to prevent it from happening to you.

Are You Interesting Enough?
The pulp and paper industry may not appear to some as a lucrative target, after all it is such an established and historic industry. What intellectual property (IP) is there that’s worth stealing? One of our customers recently exclaimed, “We’re not interesting enough for hackers.” Herein lies the issue. Today’s hackers aren’t after your IP or contact details, they’re just after your money; and one of their favorite tools is ransomware.

It is in this domain that the world has changed with the positioning of “ransomware as a service.” It is exactly as it sounds; a highly unethical practice, which sees malware being leased by hacking groups to criminal organizations. But to use it, you must abide by the rules — only targeting commercial organizations who can afford to pay.

This is where it gets surreal. Upon full payment of the ransom, these hacker groups will then altruistically offer a customer-service function that will get you back to where you were before the attack. The overriding message being “paying up = minimal disruption”! This is not a stage a company of any size would wish to reach, with prevention always recommended over repair when damage to the organization may have already harmed business, systems and reputation.

Over the past two years, incidents of ransomware have increased by over 500%. In fact, within ABB, we predict that a substantial number of our customers globally will face an attack in one form or another. Of those that have already been attacked, a high percentage could have prevented the incursion with foundational cyber control. Indeed, a few years back the question asked was, “if you will be attacked” whereas now it is more a case of asking, “when will you be attacked?”

You don’t have to go back too far to see a high-profile example of this type of attack. The May 2021 Colonial Pipeline incident saw the company’s IT system frozen out, completely crippling fuel deliveries up and down the east coast of the USA. Although the company acted quickly to try and segregate the malicious code, the damage had already been done and, once publicized, hoarding and panic buying started.

Colonial took the decision to pay the ransom — some $5 million (some of which has been recovered) — almost immediately, with CEO Joseph Blount Jr. explaining to a senate committee that he wanted “to have every tool available to swiftly get the pipeline back up and running,” before adding that “it was one of the toughest decisions of my life.”

Malware Propagation
So, how does this affect the pulp and
paper industry? If you are a commercial company with a profit flow, you can guarantee that you are interesting enough. It really is as simple as that. The chances are you might not even be singled out nor individually targeted.

The entire mill IT/automation infrastructure is only as strong as the weakest link. It could be through a USB key, an email link, or an unsecured hotspot, but once compromised only one mission system needs to be taken out to impact the entire enterprise. The Colonial Pipeline incursion was believed to be via a legacy VPN profile, which was not protected by two-factor authentication.

The pulp and paper sector traditionally holds a very low inventory, given there is no value in keeping a year’s worth of tissue/boxes. With paper being a critical infrastructure to the US economy, hacking just one tissue supplier could take out 22 percent of the capacity. Small failures could see huge effects on everything from facemasks, through to pizza and Amazon boxes, and onto building supplies.

Security Over and Above Standards

National and international cyber security legislation and standards are in place, such as the ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems. But these standards should only be considered as the foundation of any security system. A more holistic approach is required, coupled with a real understanding of what is behind this legislation, especially how systems should be configured, deployed, and maintained.

There is a big difference between best practice and what you actually need to do; a single standard cannot prescribe solutions for such a diverse range of target industries. Process industries customers, and not just those in pulp and paper, are always asking us how they can comply, recognizing that the legislation is not prescriptive enough. Cyber resilience is the ability to plan, respond and recover from cyber-attacks and data breaches, while continuing to work effectively.

Legislation + Actual Intervention

This legislation surrounding your operations needs to be considered, in parallel, with a full security audit, including an inventory of what something is, where it is and most importantly in this instance, what it is connected to. Pulp and paper mills typically have very layered networks with smart components close to the processes. Having a full device inventory is essential, together with an assessment of its current state and knowledge on what should be protected. Network segmentation can also go some way in protecting IT and OT architecture.

Foundation control is by far one of the most efficient measures any company should undertake and is a primary strategy that should be in place to maintain security postures. It can include relatively simple operations such as security patch updates, robust-antivirus installation, regular and structured backups, and network segmentation.

A bit like a mill’s network structure, your approach to cyber security — applicable for both IT and OT assets — can also be layered. Starting at asset level, you need to consider the device-level security, which for a PC would be anti-virus software that is patched and updated to its latest version number. The next layer, which could comprise PLCs or servers, should also be patched to the latest software version, along with any vendor-specific maintenance patches. To control access, you then need to ensure that adequate account management procedures are in place and that staff rigidly follow these. Next would be computer policies and hardware registers — what can and cannot be
attached to the network and to the assets.

Then we get to the firewall level, which is an interesting illustration of the inadequacies of existing cybersecurity legislation. Many documents mandate the existence of firewalls, but then go into very little detail as to their role and operation. Without configuring a firewall correctly, patching it and defining secure pathways all you are doing is box ticking as opposed to securing your network.

Above the firewall should sit the company policies and procedures, which dictate the minimum level of security. A full holistic security program should also mandate what needs to be done in the event of a breach and how operations should be recovered and bought back into action as soon as possible. Finally, above all of this lies physical security, which should prevent any unauthorized access based on site/office entry procedures.

As with any security protocol, the weakest link is often the employees. This is rarely intentional or malicious; they are simply looking at ways of under-complicating their jobs, so can be quite creative when it comes to circumnavigating security policies. All employees must be made aware of the implications, no matter how small the potential security breach. Daily work must be carried out while adhering to fundamental security practices around passwords, data storage and sharing, and with up-to-date awareness of potential risks.

Introducing cyber security management into industrial system operations can seem to be a major change and can be overwhelming. Therefore, early steps must work towards a solid understanding of context-specific risks and their prioritization. Effective collaboration with security capabilities between Enterprise IT and OT from the organization as well as among product suppliers, system integrators and operators is key.

People, Policies, Procedures

At ABB, from an overall approach, we recommend using people, policies, and procedures in conjunction with technology. Firstly, you must establish a foundational level of technical and organizational security controls to defend against the majority of the generic threats. Then you must undertake continuous management and maintenance of these controls, possibly adding more sophisticated controls, before finally creating a strong collaborative operation of cybersecurity controls with managed security services.

The primary messaging behind all of this is that you should not shy away from adopting new technologies just because of the potentially higher security risk. There are thousands of companies out there that have invested in new networks, smart automation and edge/IoT technologies that are secured against threats because they considered and implemented security as part of the overall transformation plan.

Help is Out There

While the risk to pulp and paper — and any manufacturing industry — is higher than what may be naturally assumed, my message is simple: do not be intimidated. You do not have to be clever to be secure, you just have to be cyber-hygienic. That means having a layered defense strategy in place.

Tackle the obvious stuff yourself and stay current — patching and applying updates really is one of the most important things you can do. After all, we’re not all car experts, but I don’t need a degree in automotive engineering to check my tire pressure or top up my washer fluid. For the more complicated routines, there are prescribed time-dependent service actions and a network of experts — much like in automation.

In the grand scheme of things, cyber security does not offer any pay-off or payback; it is much like insurance, you keep it current for peace of mind. From a financial perspective the biggest impetus should be: how much will it cost if I don’t have security? Now that’s a sobering thought.

Apala Ray is Global Cyber Security Manager, Process Industries at ABB.