Defending pulp and paper mills from cyber threats

By **Patrik Boo,** ABB global product manager

The attacker may be located thousands of miles away – or right on your own plant floor. No matter where your mill is located, a cyber security threat is close by. Every day your people, automation, data and operation are under threat from the many frightening repercussions of cyber breaches.

Whether it's malicious or an accident, a cyber security issue can harm your automation system, destroy data, hurt the environment, endanger your people and bring production to a halt. Its longer-term impact can even put your mill out of business.

No matter where your mill is located, a cyber security threat is close by

In paper mills, even a minor security breach has the potential to interrupt production for days. Operations may be at a standstill while experts travel to the site and handle the damage. In a worst case scenario, where your control system is wiped out, it may be weeks before you are able to be up and running again.

In August 2012, Saudi Aramco, Saudi Arabia's state-owned company and the world's largest oil producer, learned first-hand how devastating a cyber-attack can be. Hackers unleashed a computer virus called Shamoon that obliterated the hard drives of 30,000 of the company's corporate computers.

After conducting an analysis, US Secretary of Defence Leon Panetta called the Aramco attack a "significant escalation of the cyber threat." His words highlight what cyber experts worldwide already fear: a range of hazards including vandalism, political attacks, espionage, theft and employee misuse are putting companies at rapidly-increasing risk.

DAMAGE FROM OUTSIDE OR WITHIN

As they look for corporate targets, hackers are increasingly zeroing in on paper mills. Don't ask why, ask why not? They may be motivated by anything from casual sabotage, to revenge, to cyber-crime. One of the most disturbing aspects of cyber attacks is that individuals who have the intent to do harm but not the knowledge or resources, can now easily find code on the Internet that they can decompile and use to do real damage.

Some companies believe they are immune because they have developed a strong defence against outside threats, however if they haven't created safeguards against the problems that can be created by insiders, they are still at risk. The essential question for today's businesses is, how do you defend yourself against your own employees who may knowingly or unknowingly cause damage?

When companies have strong, sound security policies in place, and enforce them, they are closer to minimising their risks

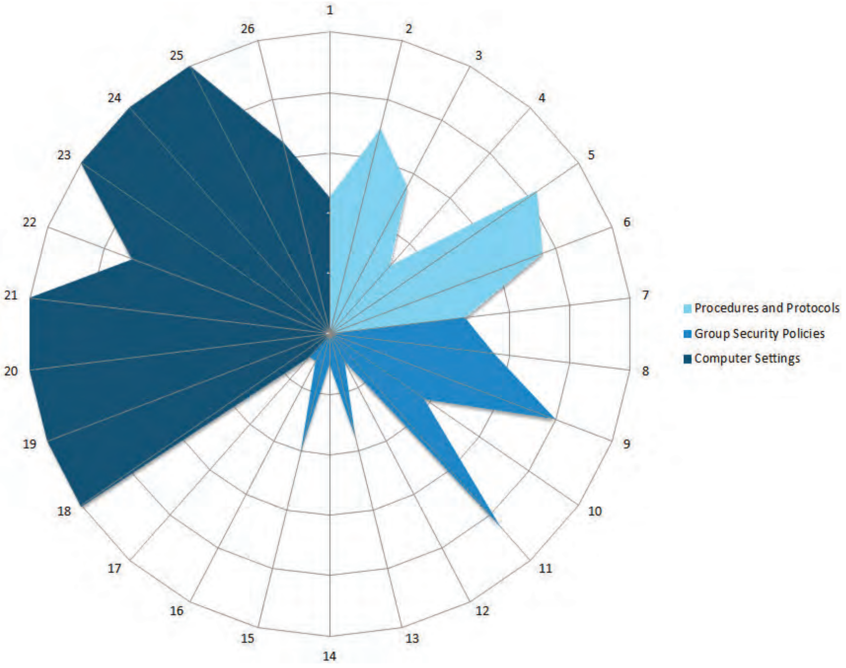

Figure 2. *The report shows the relative risk to the system based on the assessed parts. Areas with less coloring have lower risk than those with more.*

Although outside hackers are synonymous with cyber security issues, they are responsible for only a quarter of all security breaches. All of the other threats to a business are commonly caused by their own personnel.

Since many security issues can be traced to employee oversight, implementing a solid security policy and educating workers to adhere to it is key.

When companies have strong, sound security policies in place, and enforce them, they are closer to minimising their risks.

One of the easiest but most effective ways to protect your mill is by implementing awareness training for your employees. With ongoing classes, they can learn what to watch out for and why specific security policies are necessary. For example, they should not bring any outside software or USB enabled peripherals to work as they may be carrying malware.

Using your computer systems' security features is another easy safety measure. Security settings are obtainable from the control system supplier and easy to configure, and they are a sound way to protect your control system.

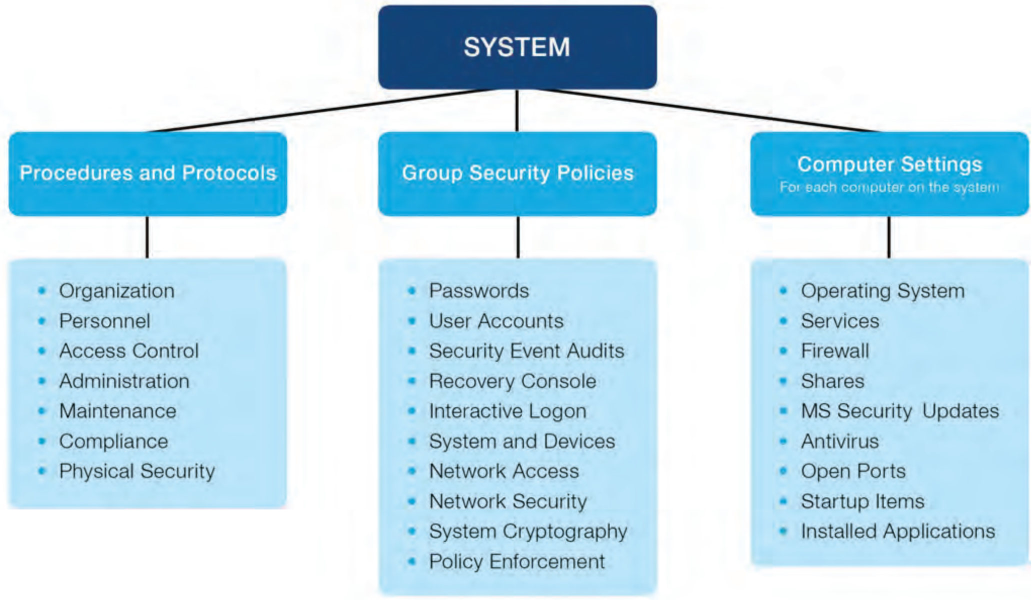

Figure 1. *ABB examines three key components of a plant's control system to determine key performance indicators.*

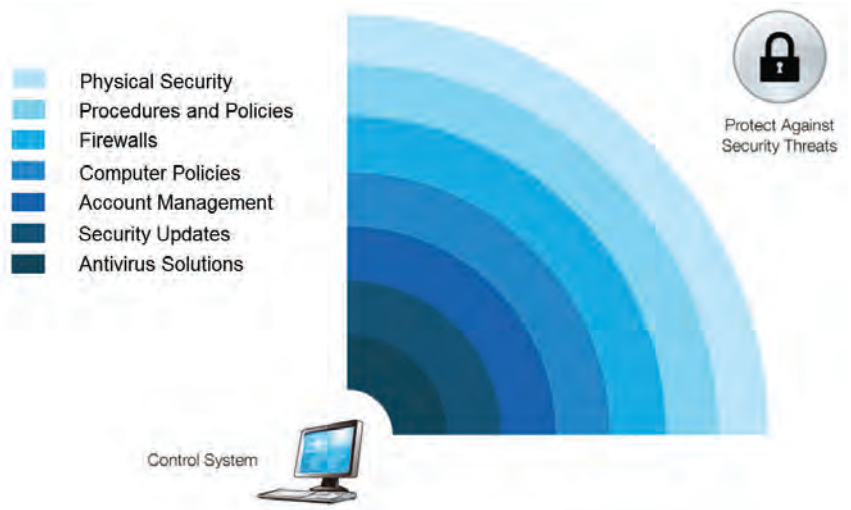

Figure 3. *Multiple layers of protection significantly reduce risk of attack*

THE AIR GAP SAFETY MYTH

Efforts to isolate a mill's control system from Internet connections are central to many papermakers' cyber security plans. As a result, mills often attempt to create air gaps – physical gaps between their control network and the Internet.

Air gaps are an appealing idea because many believe once they are in place, the control systems will be sealed off and protected from the dangers of Internet viruses or hacking. Mills often think that if they create air gaps, they are safe. However, cyber experts know that nothing, not even air gaps if they exist, can keep your control system completely isolated.

At a US Congressional hearing, held May 25, 2011, Sean McGurk, who was then Director of the Department of Homeland Security's Control System Security Department, summed it up: "In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks."

Unfortunately there are too many pathways into a mill's control system to ever make it 100 percent secure. Whether it's a misconfigured firewall, an insecure modem, infected USB keys or PLC Logic or even human, intervention, there are many channels into your control network. And those channels will leave your system open to an attack.

By focusing your mill's security efforts on only the widely known ways into your control system, you leave yourself vulnerable. A better approach is to secure your server network and the nodes that connect to it, and to train your employees so they can protect your system from security threats.

IF IT'S WORTH HAVING, IT'S WORTH STEALING

Mills invest significantly in their control systems, purchasing the hardware and software they need and spending the time and effort to customise them. If your control system is of value to you, it is of value to someone else. So it's important to protect your system no matter what.

Hackers are focusing on control systems because they can make large amounts of money by stealing your resources and trade secrets.

Competition in the paper industry is fierce, and keeping production running smoothly and product quality high are critical components to remaining competitive. A ruthless hacker with the right skills and resources has the means to disrupt both.

In paper mills, even a minor security breach has the potential to interrupt production for days

An attacker can gain unauthorised access to your control system and steal production data without your knowledge. Then they can turn around and sell that data to your competitors.

For the right price they can make production changes that are so subtle an operator may not catch them until it's too late, the paper doesn't meet customer specifications and therefore has to be scrapped.

A hacker can also blackmail mills by threatening to invade their systems, destroy their data or restrict their system access unless their demands are met. They may release ransomware, an especially vicious form of malware designed to extort money.

After the attackers prove they can disrupt your production, they will try to force your mill to make preventive payments.

MINIMISING YOUR RISKS

With all the danger presented by poor cyber security, it is essential to have a strategy to protect your mill's control system. The core of cyber security is to minimise the risks of unplanned shutdowns and disturbances, as well as health and safety issues. Although no system can be made 100 percent secure, papermakers can reduce the threat potential by developing a clear plan to protect their mill's control system. Fortunately, it is not difficult or expensive to create an effective strategy.

ABB uses the principle of combining several layers of defence to protect control systems against potential security threats, to help mills lower their risk as much as possible.

ABB's new Cyber Security Fingerprint service helps mills defend themselves against cyber attacks. ABB has extensive experience in pulp and paper projects worldwide as well as a keen understanding of what it takes to secure them, and drew on their expertise in control systems to design the Cyber Security Fingerprint.

The Fingerprint is based on an effective two-pronged approach to increase a mill's protection: ABB collects data from over 100 critical points in the system and conducts in-depth interviews with key plant personnel.

ABB uses a proprietary software-based analysis tool to analyse its findings and compare them with industry standards and best practices. After running the data, ABB calculates Key Performance Indicators in procedures and protocols, security policies and computer settings. ABB then produces a report that gives an extensive view of the mill's control system cyber security status. The report highlights both strengths and weaknesses. Importantly, it provides recommendations and an action plan for reducing cyber vulnerabilities.

Using the report as a foundation, ABB's cyber security experts will help a company develop a security strategy that is sustainable and necessary for their mill. The papermaker can also choose to have ABB implement the report's recommendations.

ABB has worked with papermakers, ranging from tissue makers to board producers, on cyber security issues for many years. Often a corporation will ask one of their mills to tighten their cyber security but the mill manager may not know how to begin. Since the Fingerprint can be used as a blueprint and starting place, it is perfect for those mills just starting to implement security measures. If a mill has a plan that's already working, ABB can help them find any elements that may be missing or that may need to be updated.

ABB's cyber security experts can be called in to help mills solve specific cyber security issues such as detecting and removing viruses. For example, a paper mill recently asked ABB to investigate why their control system was not working as it should. ABB engineers found that a virus was causing standard Microsoft Windows security functions to shut down key computer functions. ABB's cyber security experts performed anti-virus scans, discovered the compromised areas and removed the problematic components. With the issues caused by the virus eliminated, the mill's control system went back to performing smoothly.

By focusing your mill's security efforts on only the widely known ways into your control system, you leave yourself vulnerable

Most mills can benefit from a cyber status review. For example, a plant based in the Middle East recently used a Fingerprint to analyse its cyber security measures and pinpoint any gaps that could make its control systems vulnerable.

ABB's Cyber Security Fingerprint found that even though the plant already had stringent security measures in place, there were still ways that security should be tightened. Importantly, outdated and unnecessary software needed to be updated or removed. The depth of ABB's report convinced company owners to act on their findings. The result: **a more comprehensive view of the plant's safety status, better risk mitigation against cyber attacks and tighter control system security.**

Working with paper mills worldwide, ABB has found that it is never too late to begin implementing a cyber security strategy. Your mill's plan does not have to be highly complex or costly to be effective. Using smart methods, such as employee awareness training, you can lower your risk considerably. You can develop your strategy by using internal resources or you can turn to a supplier like ABB for support. But even when you feel your mill has secure measures in place, it is still critical to stay alert to potential threats and continue to work on improving your mill's cyber security.

Patrik Boo is an ABB global product manager and cyber security expert based in Westerville, Ohio. He has more than 15 years of experience in control systems engineering. Boo has a BS in Electrical Engineering from Chalmers University of Technology.