Protect your mill from cyber threats

A moment's inattention could compromise the security of your papermaking operation and make it at risk from attack through its Internet connections. PPL reports

It's a mill manager's nightmare: a cyber security breach that threatens people, automation, data and operation. Papermakers today have had to wake up to the many frightening repercussions of cyber threats.

Malicious attacks, viruses such as the Stuxnet worm, corporate espionage, unauthorized access, employee misuse, unsanctioned system modifications – an ever-widening range of hazards can put your mill at risk. And whether a cyber security incident is an attack or an accident, the impact can still be serious.

"There is one new vulnerability discovered every hour of every day," says Patrik Boo, an ABB global product manager and cyber security expert based in Westerville, Ohio.

A cyber security problem can jeopardize people's safety, destroy equipment, lose key information, hurt the environment, bring production to a standstill – and it can even put you out of business.

At the minimum, a cyber incident can turn into a significant expense. According to a 2011 study by the Ponemon Institute, the average cost of a cyber security breach is US$5.9 million.

Both hackers – and employees – can do damage

Cyber security issues that threaten businesses started to surface in the mid-1990s. In the paper industry, malware designed to harm an individual mill's control systems began appearing in 2010 – and mills were forced to begin considering the costs and hazards that a cyber attack would mean for them.

When hackers target a mill, they may be motivated by anything from casual sabotage, to revenge, to cyber crime. Boo says 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 find code on the Internet that they can decompile and use to do real damage.

The person who maliciously hacks into a company's system doesn't have to be an unknown; he or she might be a disgruntled former employee. Boo tells the story of an employee who took being fired so calmly that his manager agreed he could go back to his cubicle and pack up his belongings. The employee returned to his desk and deleted the company's most important databases, causing incalculable harm.

Competition in the paper industry can be fierce, and an unscrupulous competitor with the right computer skills could cause enormous trouble. In mills, smooth running production and high product quality are crucial – and a ruthless competitor has the means to disrupt both. A hacker can gain unauthorised access to your system to gather intelligence, steal information, or even 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 has to be scrapped.

Although hackers are synonymous with cyber security problems, Boo says they are behind only a quarter of all security breaches. Most often, the cyber problems businesses deal with are caused unintentionally by their own employees.

Worker carelessness, accidentally-passed viruses and unauthorised access create the bulk of cyber security issues. An employee who, for example, uses the system to recharge a smart phone or a USB stick can create havoc if the device has a virus they didn't know about. An operator who overrides their system access in the rush to correct a problem can trigger a cyber crisis.

"Many of our customers say, 'we don't have a problem because our control system is not connected to the Internet'," says Boo. "That's a good first step, but they also need a policy that no one can connect a phone with Internet capabilities to the system to charge it."

Creating an effective strategy

With all the danger presented by poor cyber security, creating a strategy to protect your mill's control system is essential. "The core of cyber security is to minimise the risk of unplanned shutdowns and disturbances, as well as health and safety issues," says Boo.

Although no system can be made 100 percent secure, papermakers can take measures that go a long way toward minimising risks. Having a comprehensive understanding of the current state of your mill's security and a sound plan for protecting your control system is essential for reducing the threat potential.

ABB combines several layers of defense to protect control systems against potential security threats. "We help our customers lower their risk as far as is reasonable," says Boo.

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

A proprietary software-based analysis tool is used by ABB 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 cyber security status. The report highlights both strengths and weaknesses. Importantly, it provides recommendations for reducing cyber vulnerabilities.

Using the report as a foundation, ABB’s cyber security experts could help a company develop a security strategy that is sustainable and right for their mill. The papermaker can also opt to have ABB implement the report’s recommendations. Additionally, ABB can provide scheduled security scans or implement continuous security tracking through remote connectivity.

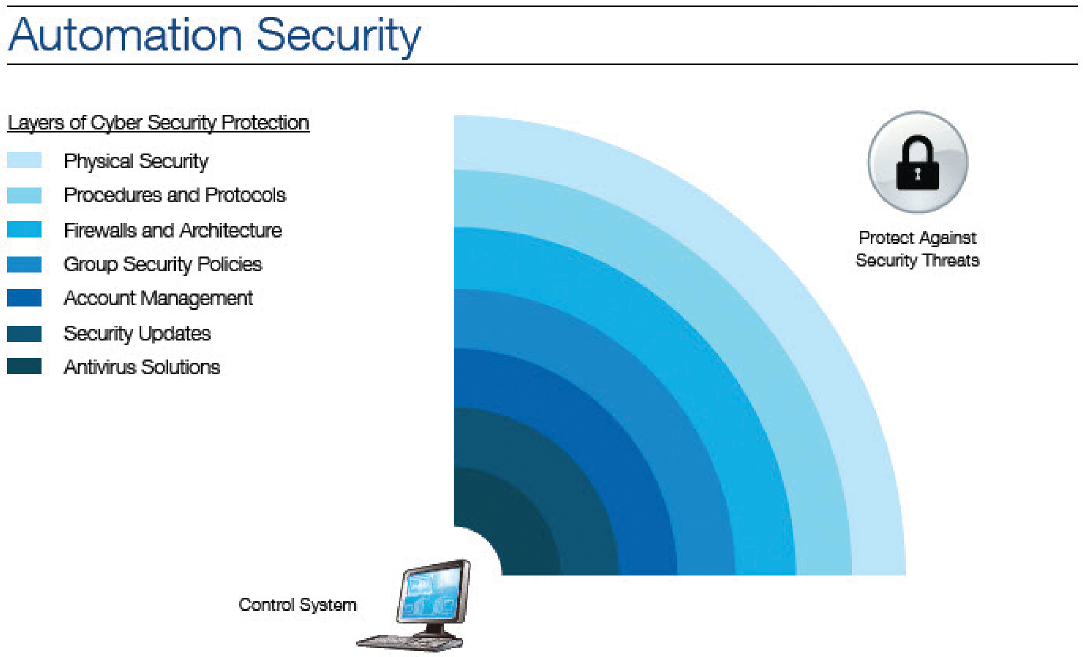

ABB uses Defence in Depth strategy that ensures multiple layers of protection

“Often a corporation asks one of their mills to tighten their cyber security and the mill manager may not know where begin. The Fingerprint is perfect for them. It’s a blueprint, it’s where you start,” explains Boo. “If a mill has a plan that’s already working, ABB can help them find cyber security measures that may be missing or that may need to be updated.”

ABB’s experts can even be used to solve very specific, unexpected cyber security problems. One example: a customer recently contacted ABB because their control system was not working as they thought it should. ABB engineers investigated and discovered that a virus triggered Microsoft Windows to shut down one of its key functions. ABB’s cyber security experts performed anti-virus scans, pinpointed the compromised areas and removed the problematic components. With the issues caused by the virus eliminated, the customer’s control system went back to performing smoothly.

Since so many security issues can be traced to employee misuse, implementing a solid plan and educating workers to adhere to it is key. The Cyber Security Fingerprint is, for example, based on the principle of least privilege – mill personnel should have only the system access that they need to perform their duties.

Says Boo: “When companies have strong, sound policies in place, and they enforce them, they are a good step closer to minimising their risks.”

More information from ABB Drives and Information Systems, 579 Executive Campus Drive, Westerville, Ohio 43082, USA. Tel: 1 614 818 6300.

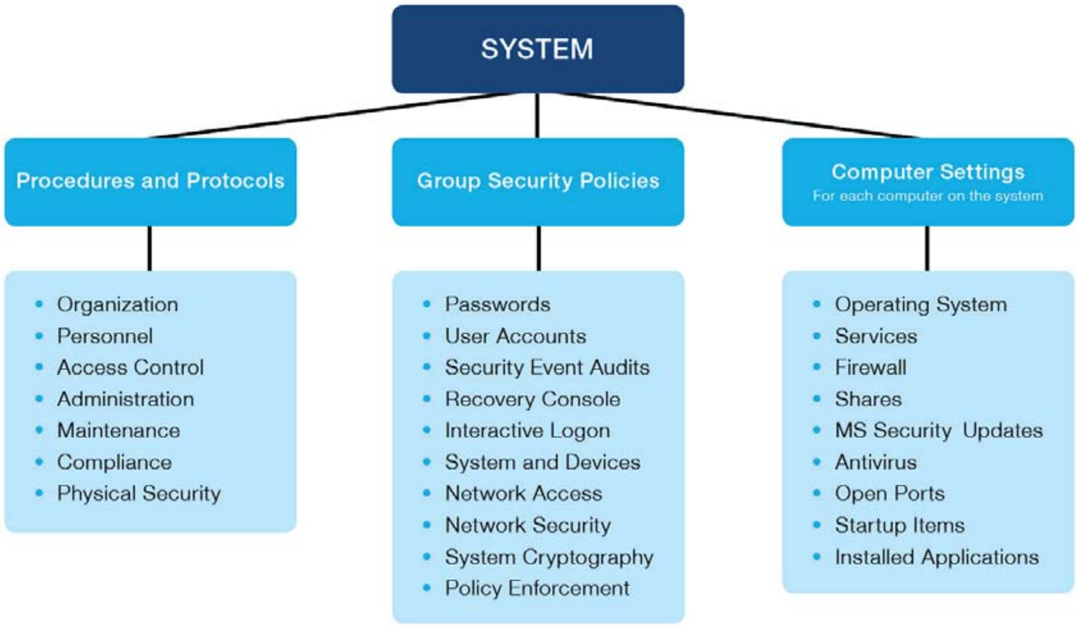

ABB examines three key components of a plant’s control system to determine key performance indicators