Hewlett Packard Enterprise

Business white paper

# Clear the floor of threats

What the steel industry needs to know about cyber security

# Table of contents

Security measures at steel plants used to encompass gates and armed guards, but now cyber security is moving to the forefront as cyber threats within the industry grow. Whether threats are internal or external, malicious or unintentional, you need to see and understand threats earlier so you can respond and remediate faster.

Preventing cyber security breaches is difficult. Breaches come from a growing variety of sources: IT system attacks and intrusions, unauthorized system activity, malicious software, industrial and nation-state espionage (via advanced persistent threats), and any other access, manipulation, or deletion of information and data. Many breaches are so subtle in nature that an overwhelming majority go undetected—sometimes for years or until a third party notifies the enterprise.

In today's environment, it's no longer a question of whether you will suffer a security breach. You will. This is simply an artifact of the hyper-connected, technology-driven world we live in. But will you be prepared to respond with confidence and minimize the damage?

HPE, with its in-depth knowledge of the steel industry and ISA/IEC-62443 control standards, can help you establish the processes and procedures for an optimal approach to breach management. Whether you've had a breach or want to create an effective response capability, we'll collaborate with you to limit impact, close vulnerabilities, and minimize the risk of future events.

## Cost of a breach

The impact of a breach can be enormous. According to the Ponemon Institute, "the average annualized cost of cybercrime for 56 organizations in our study is $8.9 million per year, with a range of $1.4 million to $46 million. On average, the companies in the study suffered 1.8 successful attacks per company per week."[1] These costs do not include disruption to operations or damage to relationships with customers or investors. They do not include the steep financial penalties associated with compliance or breach notification laws. And they do not include costs associated with litigation for damage caused by the attacks.

In the steel industry, with its reliance on automation and industrial controls, a successful hacker could potentially tamper with the formula for making steel or disrupt machinery, manufacturing systems, and processes. If the wrong material goes into the furnace or the process timing is off, that could affect the integrity of the steel that is produced. If the hacked steel makes it out into the field and causes damage, the litigation costs could be astronomical. And, in the aftermath, the damage to the company's brand and lost business could be devastating.

All in all, the cost of a breach will likely exceed the cost of preparation and prevention. Although the cost per breach has been rising, the Ponemon Institute study also found, "companies that invest in adequate resources, appoint a high-level security leader, and employ certified or expert staff have cybercrime costs that are lower than companies that have not implemented these practices."[2]

[1] Ponemon Institute, "2012 Cost of Cyber Crime Study: United States," October, 2012.

[2] Ibid.

## What makes a steel mill a target?

Groups such as environmental "hacktivists" may choose to attack a steel mill for the simple reason that steel mills are highly visible producers of carbon. Or they may choose to attack because steel is a key component of the pipes, tubes, and other equipment required for oil drilling or hydraulic fracturing (fracking). Although many consider transportation, financial networks, or nuclear power plants to be prime targets, malicious hackers are likely to attack the targets that are most vulnerable. If steel mills don't have adequate protection, they are left as targets of opportunity, and the effects are potentially devastating.

Steel mills, as a component of America's critical infrastructure and industry, are also a target of corporate and international nation state-sponsored espionage, seeking to steal trade secrets or gain a competitive edge in the global market. Protecting your valuable intellectual property and competitive advantage must be a priority.

But threats can also come from much closer to home. A disgruntled employee or former employees from anywhere along the supply chain could cause significant damage, or take your trade secrets with them and move on to a competitor. Employees without adequate security knowledge become unwitting targets and create avenues for infiltration into the corporation. Workers who share passwords over email or write passwords down to remember them can inadvertently create vulnerabilities that can't be mitigated with a simple technology fix.

## Security threats on the shop floor

As technology proliferates on the shop floor, so does the potential for security vulnerabilities. Today, there are typically thousands of electronic devices on the floor for a single mill, and managing all these devices can be a huge challenge. Often the devices are configured and deployed by an industrial automation vendor who is the subcontractor in a larger project, such as the renovation of a line.

It is not unusual for the shop owner to take delivery without an inventory of the devices or any management tools in place to track them. This causes problems because you can't protect what you can't manage—or worse, what you don't know is present. If you can't identify which devices you have, then you can't identify which devices belong on your network, and you can't distinguish which devices might be associated with malicious intruders.

Organizations that find themselves in a situation such as this require an immediate "state of the network" assessment for present vulnerabilities or even active threats. This should be followed by a plan to operationalize the tracking and management of connected assets on their floors. If you are planning the renovation of a line, you can avoid this situation by building in security and deploying management tools for your new devices. We also recommend having a third-party security organization independently verify your design, configuration, and response capabilities.

It is common for plant engineering or manufacturing engineering to sanction the installation of unmanaged IT equipment—such as PCs and network devices—that is unknown to corporate IT and, therefore, unmanaged by corporate IT. Much like on corporate networks, this "shadow IT" is difficult to avoid but possible to manage with a strategic tracking and management program in place.

In addition to the devices that are part of the line, employees increasingly want to bring their personal mobile devices to work. To get their devices to work, employees will bypass unenforced device policies—without the knowledge, permission, or monitoring of the IT department and without security protections in place. An unlocked door is an easy target for a burglar. And employees can expose the company through rogue networks and attached

devices that create vulnerabilities that malicious attackers can easily exploit to get to the assets they want.

Existing corporate security mandates don't necessarily address these issues. Attackers are often part of a global underground network that shares the latest information about vulnerabilities and attack techniques. Meanwhile, the bureaucracies that develop compliance mandates and corporate security policies may be up to two years behind the reality on the ground. Furthermore, the litigious culture in the industry makes information sharing, even in close circles, a difficult task. This means that if you are only compliant with current regulations, you are falling behind. Given the blistering pace of technology and attackers' ability to exploit it, you literally cannot afford to play catch-up.

In addition, there can be a difference between corporate security policy and the way things actually operate on a plant floor. Corporate security mandates may not address the problems you face on the shop floor and may hamper your ability to get your job done.

While it's impossible to lock everything down and still function properly, your employees and supply chain partners need to be able to share, collaborate, and openly exchange data where it makes sense. Ensuring your security organization is strategically supporting your business is paramount to creating a smoothly operating and safe environment.

## Fragmented security approach perpetuates failures

Like most organizations around the world, many steel producers take a fragmented approach to cyber security. They often respond to each threat by installing a new technical control or point solution. Common point solutions include identity and access management, anti- malware, anti-spyware, network security appliances, and self-serve security incident response. Each of these solutions requires time, resources, and funding to fine-tune, maintain, and keep up with necessary updates. This situation becomes untenable because there are too many threats to chase, too many point tools to maintain, and too many opportunities for attackers to exploit—created by the lag between the rapidly evolving threats and the security technologies employed to defend against them.

This fragmented approach rapidly consumes budget and time. It leaves few resources to keep up with rapid changes in business drivers that bring more strategic advantages, such as modernizing applications or building new plants. If you find yourself only reacting to the latest threat, you may be caught in a never-ending cycle of solutions that never really solve your security issues but create more busy work for your strained resources.

Although point solutions serve a valuable purpose, and are, in some cases, the most viable approach, you need to look at the bigger picture. Engaging the right point solutions and the right services to help you make it all work more effectively together is critical. Furthermore, industry experts can help you manage the security ecosystem and enable you to move from what feels like "whack-a-mole" (a forever-reactive security model) to a proactive approach. This lets you focus on a strong strategy, mitigation impact through detection, rapid response, and the ability to quickly restore affected services.

As factories continue to automate and modernize, shop floors are quickly becoming integrated with front- and back-office computer networks. This means that your receptionist may be on the same physical network as one of your critical industrial systems that control the production line. Properly architected networks are segmented and compartmentalized but still effectively communicate and serve their intended purposes.

**Understand. Detect. Respond. Restore.**
Get on with business. At HPE, we believe that the most effective way to protect your plant is to take a four-pronged approach to breach management. These are the four areas you need to focus on to become a more effective security organization.

- Understand: You need to define an overall security strategy that will enable you to detect, respond to, and restore services from attacks. Your strategy should address planning, risk assessment, and controls—not only prevention. To begin, you need to understand the scope of the network and devices that need to be protected.
- Detect: Early detection limits the damage caused by an attack. After you have a clear and defined strategy, you need to make sure you can monitor and detect potentially damaging activity.
- Respond: Rapid, effective, and purposeful response is critical when addressing a detected issue in your environment. We recommend developing and maintaining capabilities that let you figure out what attackers might do and close off any opportunities they might exploit. This includes implementing stop-gap measures, shutting down avenues of attack, and preserving evidence while restoring critical business services.
- Restore: The single most critical thing the information security organization can do when facing a breach or intrusion is to restore business-critical services in a meaningful and timely manner. While conducting investigations into the root cause of an incident, it's important to understand the chain of events as well as the full scope of the intrusion. However, the business is primarily interested in one thing: restoring services. Without critical services such as networking or industrial control systems managing shop floors, the continuation of business becomes impossible.

In today's environment, where threats exist from malicious attackers as well as internal sources, it is highly likely that your organization will suffer from a security breach. In fact, you may have already experienced one—or several—without knowing it. Most organizations don't realize a breach has happened until it is uncovered by other efforts.

Developing a clear approach to breach management is no longer a "nice to have." To remain competitive, you must adapt to the changing threat landscape. To do this, you must develop a comprehensive strategy that defines what needs to be done before a breach, what to do when an attack occurs, and how to address the quickly evolving legal and compliance requirements.

To keep your steel mill safe and operating smoothly, you should establish a proactive security posture that enables you to secure your information while improving the flow of that information throughout the enterprise—enabling innovation, improving collaboration, and increasing competitiveness.

## Gain the HPE advantage

- HPE has the industry's most complete portfolio of services—from design, architecture, and preparedness assistance to critical response services.
- We can help you monitor and test for vulnerabilities, detect and respond to active intrusions, and restore critical services.
- HPE is vendor neutral when it comes to security products, ensuring you always get the optimal solution for your situation.
- We have broad experience in the manufacturing industry in general and the steel industry in particular.
- HPE has extensive experience with the ISA/IEC- 62443 control standard for industrial security.

Learn more at
hp.com/enterprise/manufacturing

**Sign up for updates**

★ Rate this document

Hewlett Packard Enterprise



4AA4-6483ENW, November 2015, Rev. 1