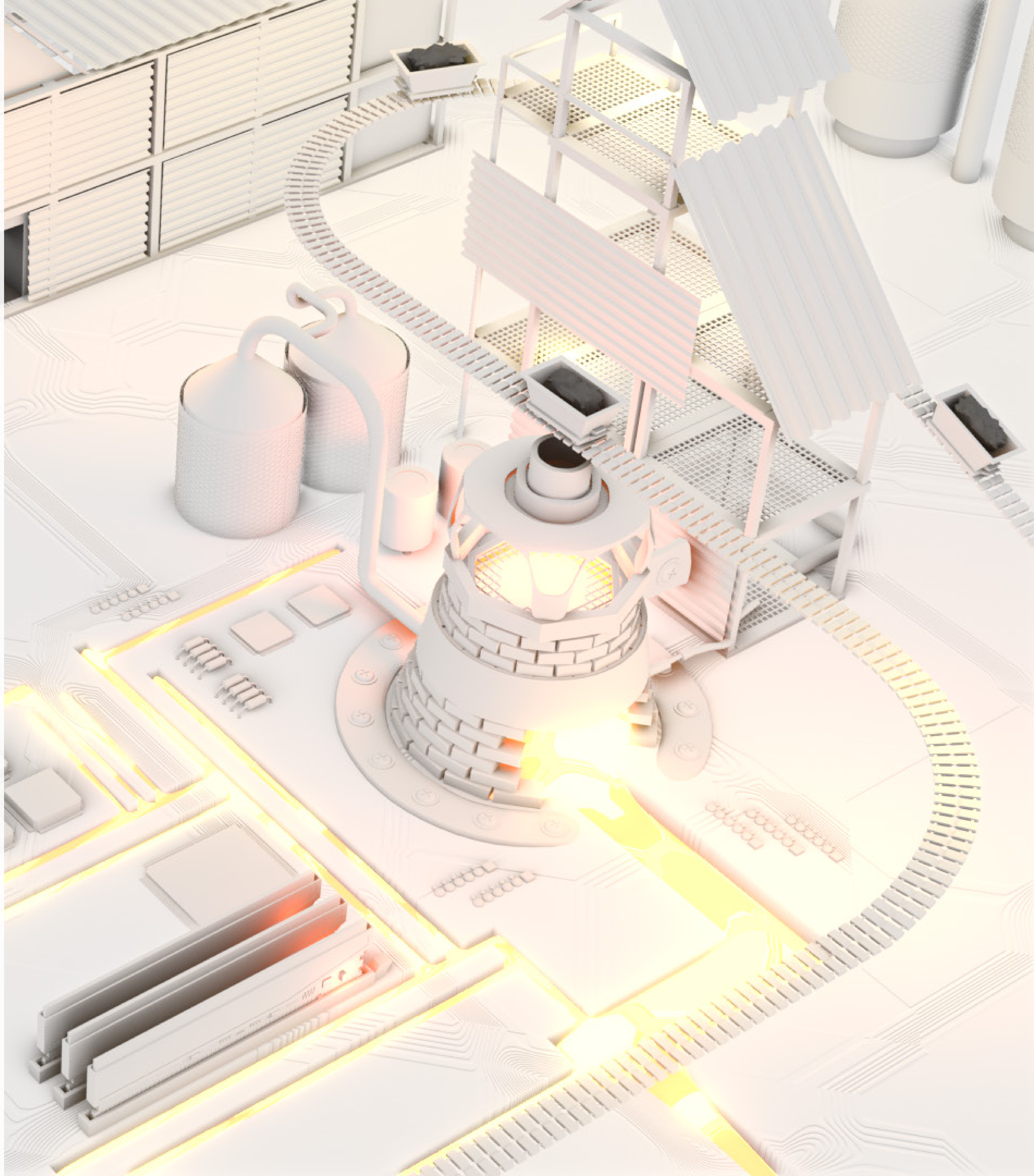
Cyber Case Study

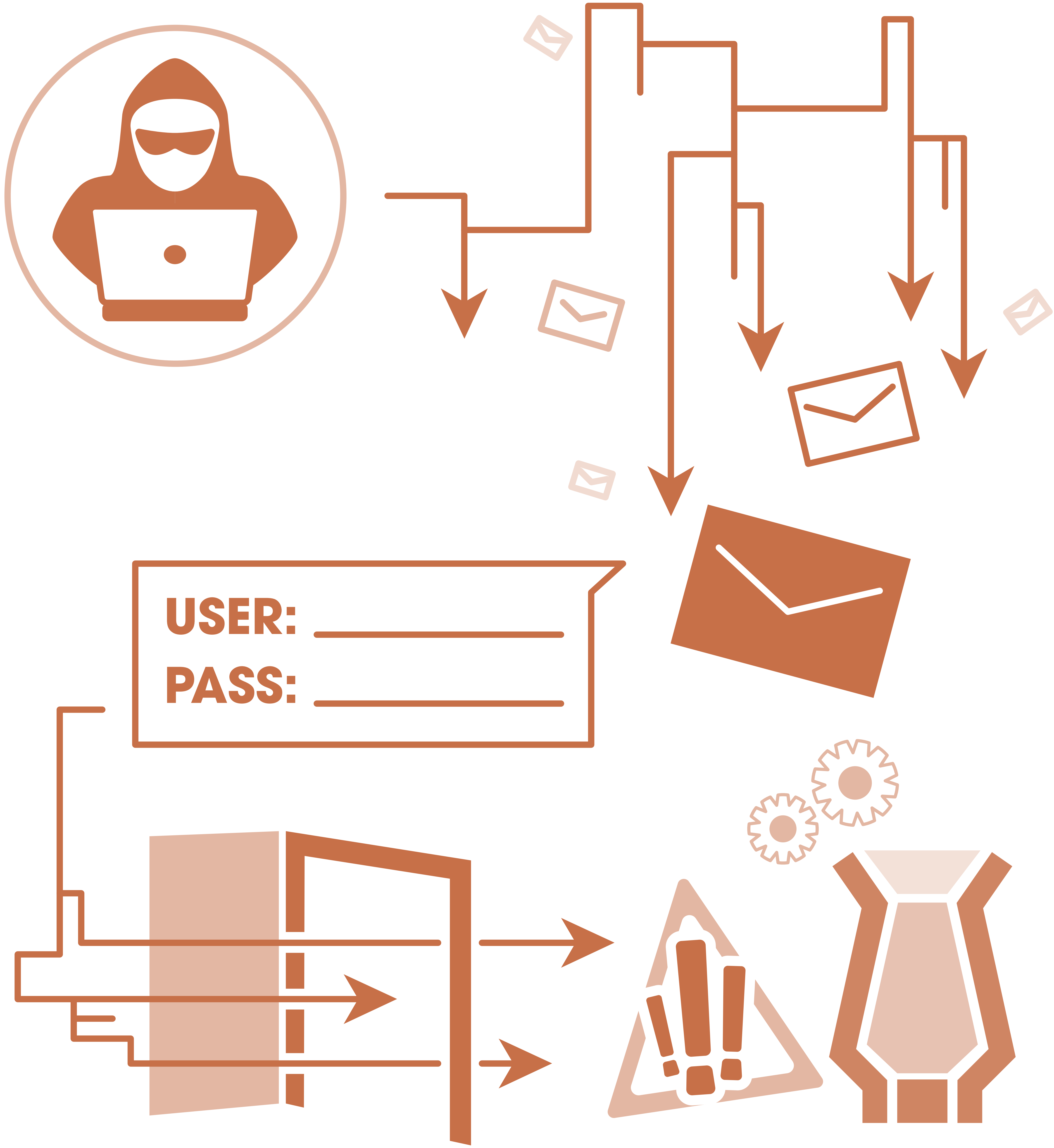
provided by MST Insurance Solutions, Inc.

Hack at Steel Mill Causes Physical Damage

In late 2014, the German Federal Office for Information Security (BSI) released a report detailing a disruptive cyberattack at an unnamedsteel mill facility. The attack—which was deployed through a combination of social engineering tactics and malware—compromised several of the steel mill's industrial control components. From there, equipment breakdowns and production outages ensued, resulting in extensive property destruction.

This attack has become known as one of the first cyber incidents to result in significant physical damage—demonstrating the widespread losses that such incidents can cause. In hindsight, there are various cybersecurity lessons that organizations can learn by reviewing the details of this incident, its impact and the mistakes the facility made along the way. Here's what your organization needs to know.





The Details

The BSI's 2014 report explained that a large-scale cyberattack occurred at an undisclosed steel mill facility in Germany earlier that year. The attack initially stemmed from cyber-criminals using a range of social engineering techniques—namely, spear-phishing emails—to manipulate some of the facility's employees into exposing their security credentials. By impersonating a trusted source within the facility, the cybercriminals successfully tricked multiple employees into viewing fraudulent emails. Opening the emails triggered the launch of a malware program that extracted the employees' usernames and passwords.

The cybercriminals then gained access to the steel mill facility's office network and production systems using these stolen credentials. Once the cybercriminals infiltrated the facility's operational technology, they began targeting specific industrial control components and interfering with the functions of certain machinery and equipment—thus contributing to production failures. In particular, a blast furnace at the facility was unable to be shut down properly. These incorrect shutdown protocols proved detrimental to the furnace, causing substantial physical damage at the facility.

The perpetrators of this incident remain at large, and their true motivation for the attack is still unknown. However, the BSI's report confirmed that these cyber-criminals possessed an abundance of technical knowledge—both in the realm of traditional IT systems and the steel mill facility's specialized, industry-specific technology. As such, cybersecurity experts have proposed that the perpetrators may have previously worked within the steel industry or belonged to an advanced group of cybercriminals.

The Impact

Because the name of the steel mill facility and specific information regarding their operations were never shared, the full impact of this cyberattack is undetermined.

Nevertheless, the facility likely faced the following consequences from the incident.

Physical destruction

The BSI's report explained that the improper shutdown of the blast furnace led to "massive" property damage at the steel mill facility. Fortunately, no employees or members of the public were injured by this incident. Yet, given the fact that a blast furnace usually holds molten metal heated to extreme temperatures, it can be deduced that any malfunction or breakdown of this equipment contributed to severe physical destruction—impacting both the furnace itself and any property nearby. Affected property could include additional machinery, equipment and structural elements of the facility (e.g., walls, floors and piping).

Recovery expenses

As a result of physical damage from the cyberattack, the steel mill facility undoubtedly encountered substantial recovery expenses. Although the complete list of facility components, specialized equipment and production systems that were impacted by the incident is unclear, the cost of repairing a blast furnace alone is typically millions of dollars—enough to wreak financial havoc on any organization.

Significant disruptions

Apart from physical destruction, cybercriminals interfering with the steel mill facility's operational technology and causing subsequent outages undoubtedly led to large-scale disruptions. After all, the facility essentially lost control of its production operations throughout the attack. Even after the attack concluded, the facility likely experienced delays in the process of recovering compromised components and attempting to resume normal operations.

The BSI's report explained that the improper shutdown of the blast furnace led to **"massive" property damage** at the steel mill facility.

Although the complete list of facility components, specialized equipment and production systems that were impacted by the incident is unclear, the cost of repairing a blast furnace alone is typically **millions of dollars—** enough to wreak financial havoc on any organization.

Lessons Learned

There are several cybersecurity takeaways from the attack at the steel mill facility. Specifically, the incident emphasized these critical lessons:

Employees are a key line of defense.
If the steel mill facility's staff had known not to open the cybercriminals' malicious emails, this incident likely could have been prevented altogether. With this in mind, it's vital for all employees to receive sufficient workplace cybersecurity training. Knowing how to detect and respond to potential cyber threats—such as phishing scams—can help employees stop cybercriminals in their tracks. Specifically, employees should be educated on these security best practices:

- Avoid opening or responding to emails from unfamiliar individuals or organizations. If an email claims to be from a trusted source, verify their identity by double-checking the address.
- Never click on suspicious links or pop-ups—whether they're in an email or on a website. Don't download attachments or software programs from unknown sources or locations.
- Utilize unique, complicated passwords for all workplace accounts. Never share credentials or other sensitive information online.
- Only browse safe and secure websites on workplace devices. Refrain from using these devices for personal browsing.

Contact a supervisor or the IT department if suspicious activity arises.

Effective security software is critical.
In addition to employee training, a wide range of security software could have helped the steel mill facility detect, mitigate and potentially prevent this attack. Although this software may seem like an expensive investment, it's well worth it to avoid devastating cyber incidents. Necessary security software to consider includes network monitoring systems, antivirus programs, endpoint detection products and patch management tools. This software should be utilized on all workplace technology components and updated regularly to ensure effectiveness. Also, it's valuable to conduct routine penetration testing to determine whether this software possesses av ny security gaps or ongoing vulnerabilities. If such testing reveals any problems, these issues should be addressed immediately.

Physical exposures must be considered.
Prior to this incident, it's safe to say that most organizations didn't include physical exposures within their cyber risk assessments. But, this attack showcased that such liabilities shouldn't be ignored. It's critical to consider whether any physical elements of your organization's operations could be vulnerable when evaluating its cyber-risks, and introduce effective loss control measures to minimize these concerns. Further, the potential for physical damages should be carefully reviewed when your organization outlines various attack scenarios and mitigation protocols in its cyber incident response plan. It's best to map out how workplace technology is connected to physical processes or components within the organization in order to detect these exposures.

Proper coverage can offer the ultimate protection.
Finally, this attack made it clear that no organization is immune to cyber-related losses—both digital and physical. That's why it's crucial to ensure adequate protection against all forms of cyber-related losses by securing proper coverage. Make sure your organization works with a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, **contact us today.**