Biden Warns of Imminent Cyberattacks and New Regulations — Is Your Business Prepared?

The law firm of Tucker Arensberg contributes this quarterly column focused on the legal issues that may impact our readers. Tucker Arensberg is a full-service law firm headquartered in Pittsburgh, Pa., USA. Servicing the legal needs of the iron and steel industry, Tucker Arensberg has also provided legal counsel to the Association for Iron & Steel Technology.

Author

Alexandra N. Boyer
Associate, Tucker Arensberg Attorneys,
Pittsburgh, Pa., USA
+1.412.594.3924

TUCKER ARENSBERG
Attorneys

If you have any questions about this topic or any other legal topics, contact attorney Thomas P. Peterson at +1.412.594.3914 or tpeterson@tuckerlaw.com. Please include your full name, company name, mailing address and email address in all correspondence.

Views expressed in Legal Perspectives do not necessarily reflect those of *Iron & Steel Technology.*

The war in Ukraine and the high-profile cyberattacks on SolarWinds and the Colonial Pipeline have renewed focus on the cybersecurity of the United States' vital businesses, such as the steel industry. To help strengthen the government's ability to respond to these attacks, President Joe Biden signed into law the Strengthening American Cybersecurity Act of 2022. The Act imposes new duties upon companies to report cyberattacks and ransomware payments to the federal government within 24 or 72 hours.

The steel industry, as a vital component of U.S. infrastructure and military, is a target for foreign governments to sabotage and for criminals to hold hostage for ransom. Manufacturing processes use open platforms and common operating systems, which cyberattackers may seize to disrupt production, damage equipment or steal intellectual property. Therefore, preparation and knowledge are key to protecting your company. This article will provide background on different kinds of cyberattacks and how to best respond under the new Act.

What is a Cyberattack?

We often hear of identity breaches in the news or see hackers in movies, but exactly is a cyberattack? The Computer Security Resource Center at the National Institute of Standards and Technology defines a cyberattack as an attack "for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure or destroying the integrity of the data or stealing controlled information."[1] Many forms of cyberattacks require software to be installed which allows the hacker to access or control the company's data or operating systems. This software is typically referred to as malware. A few common forms of cyberattacks include denial-of-service (DoS) attacks, ransomware, brute force password attacks and domain name system (DNS) spoofing.

Denial of Service Attack — A DoS attack purposefully overwhelms an operating system to the point where the system shuts down. A hacker creates malware which floods the operating system with so many requests for service that the operating system cannot keep up. This can result in a disruption of your business or can be used to create vulnerabilities in which to slip malware into your company's operating system.

Ransomware — Ransomware is a malicious software "designed to encrypt files on a device, rendering any files and the systems that rely on them unusable" to the rightful owner or user.[2] A criminal then demands payment, usually in the form of cryptocurrency, to decrypt the files. There has been a growing number of ransomware attacks on companies, most notably the Colonial Pipeline attack in 2021. A Russian cybercrime organization, known as DarkSide, used a password from an old account to access Colonial Pipeline's servers and lock the company out. Although the FBI does not recommend paying ransoms, Colonial Pipe paid US$4.4 million through Bitcoin to regain control. Colonial Pipeline estimated that it will take tens of millions of dollars to completely restore its servers, but the damage it caused to their reputation is beyond comprehension.[3]

Brute Force Password Attack — This kind of cyberattack is seen in movies, where the hacker either guesses the password or uses a program to run many different passwords until one works.

DNS Spoofing — In this kind of attack, a hacker creates a fake or “spoofed” website that looks like the target’s legitimate site and alters the real website to secretly send users to the spoofed website instead. Once on the spoofed site, the unwitting user enters their username and password into the fake login, letting the hacker learn the combination. The hacker can then use their username and password on the real website to gain inside access to the company.

How Do I Prevent a Cyberattack?

The key to preventing a cyberattack is preparation and mitigation. The FBI and The Cybersecurity and Infrastructure Security Agency (CISA) recommend implementing the following:

Back Up Data — If you experience a cyberattack, a backup of your data helps to ease the pain of the attack and may allow your company to recover faster. Make sure that the backup is offline and encrypted so that it is not also vulnerable to attacks. Many forms of ransomware purposefully attempt to locate backups and delete them.

Update the System — Although it feels like a chore, keeping your hardware and software up to date to protect against the latest cyberattacks and vulnerabilities is the easiest way to prevent cybercrime.

Use Multi-Factor Authentication — A multi-factor authentication plan is a security process in which users provide multiple, different credentials before they are allowed access. In general, users only provide one kind of credential, typically an alphanumerical password, before they can access sensitive data or accounts. In a multi-factor authentication plan, users must provide another token or password before they can access the servers.

Some multi-factor authentication plans use biometric factors, such as a fingerprint or retinal scan, while others use a location factor, in which access may only be permitted within certain geographical boundaries. This helps to prevent attacks from overseas groups or governments who are not physically close to the target servers.

Lock-Out Multiple Password Attempts — To prevent a brute force password attack, implement a policy where users are only permitted a certain number of attempts to enter a password before they are locked out and prevented from trying to log in.

Designate a Crisis Response Team — In the event of a cyberattack, choose a group of employees who will respond to the attack. Having a response team in place saves precious time at the start of a cyberattack. Designate roles and delegate authority to prevent confusion or in-fighting. Keep a list of how to contact the response team at any time, as well as a list of contractors and providers who should be alerted.

Talk to the Experts — Because the steel industry is a critical infrastructure organization, CISA and Department of Homeland Security offer free cybersecurity assessments. Email vulnerability_info@cisa.dhs.gov to get started.

I’ve Experienced a Cyberattack — What Now?

If you fall victim to a cyberattack, act immediately to prevent further harm to your company. CISA recommends the following steps:

Detect the Malware — Someone in your Crisis Response Team should be tasked with locating and isolating the source of the malware. Once the malware is located, immediately take the impacted systems offline to prevent further damage. If you cannot find the malware, shut the entire system down.

Inspect the Damage — Take note of what systems have been impacted by the breach and prioritize which systems to restore first. Attempt to find associated users or programs that may still contain the malware.

Contact Law Enforcement — Because the steel industry is a critical infrastructure organization, the Act requires that you preserve all data related to the cyberattack and report it to CISA within 72 hours. If a ransom is paid, it must be reported to CISA within 24 hours. These reports must contain a description of the attack, potential vulnerabilities exposed, tactics used, impact of the cyberattack to business operations, and the amount of ransom paid, if any.

Failure to report a cyberattack or ransom paid could result in penalties to the company, and the Department of Homeland Security may subpoena information and work with the Justice Department to ensure compliance. However, companies who file a report under this Act are immune to any civil suit arising from the report.

If sensitive data, such as confidential identity information or banking and financial information, was breached, you may be obligated to report it to the

Federal Trade Commission and your state's Attorney General or Bureau of Consumer Protection.

The Next Steps

The new 24- or 72-hour time limit in the Act is a short window of time to investigate, gather necessary information, and make a report, so advanced preparation is key. Companies should start by creating the necessary procedures to comply with the new regulations now and prepare to protect your company from future cyberattacks.

References

1. https://csrc.nist.gov/glossary/term/cyber_attack.
2. https://www.cisa.gov/stopransomware/ransomware-101.
3. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.