Export Compliance Manager

THE CONVERGENCE OF CYBERSECURITY AND EXPORT CONTROLS AND SANCTIONS ENFORCEMENT

DoJ: Export controls no excuse for employment discrimination

Seagate: Largest-ever penalty ushers in new era of BIS enforcement

6 ways to make your ICP more efficient without breaking the bank

The notion of circumvention under EU sanctions

Issue 33. MAY 2023

The convergence of cybersecurity and export control/sanctions enforcement

The cyberthreat environment continues to grow more menacing. Over the last year, organizations have been faced with a weekly, if not daily, deluge of ominous cybersecurity alerts and advisories from law enforcement. Cyberattacks come in many forms – malware-based attacks, phishing, spoofing, zero-day exploits, denial-of-service attacks, supply chain attacks, and insider threats, among others – and are clearly on the rise. No organization is immune. Indeed, over the last year, the vast majority of companies experienced some form of a cyberattack.[1] Accordingly, it is not matter of *if* your organization will experience a cyberattack but *when*, and what you can do to minimize liability risks.

> It is not matter of *if* your organization will experience a cyberattack but *when*, and what you can do to minimize liability risks.

Export controls applicable to cybersecurity items and services

While this increased cyberthreat ecosystem has resulted in increased liability risks for numerous companies, it has also created business opportunities for cybersecurity companies. These companies should consult the export control regulations before selling cybersecurity services or items to a foreign person or foreign entity. Hacking services that benefit a foreign government constitute defense services, which are controlled under Category XI of the US Munitions List for which authorization from the State Department would be required in the form of a Technical Assistance Agreement. In 2021, three former NSA employees entered into a deferred prosecution agreement with the Department of Justice ("DOJ") and paid more than $1.6 million to resolve charges that they carried out computer network exploitation and intelligence gathering operations for the United Arab Emirates government.

Similarly, "cybersecurity items" that can be used for mass surveillance, espionage, and other malicious purposes are controlled under the Department of Commerce's Cyber Rule, which went into effect in May 2022. Included within this rule is the "export of delivery or command and control tools (hardware and software), as well as the export of technical data for developing exploits (intrusion software)."[2] Commerce's Cyber Rule created a new license exception – the Authorized Cybersecurity Exports ("ACE").[3] ACE allows the export of cybersecurity items for vulnerability disclosure or cyber incident response as long as the item does not contain encryption and is not being exported to

[1] Although the numbers are imprecise, numerous studies and reports have concluded that more than 50% of companies have experienced some form of a cyberattack in the last 12 months and one study found that 94% of organizations across 14 countries experienced a cyberattack in the last year. See Sophos Whitepaper, published 4 April 2023 available at sophos-the-state-of-cybersecurity-2023-wp.pdf.

[2] Commerce Cyber Rule FAQs n.15 at 10.

[3] See 15 C.F.R. § 740.22.

[4] See 15 C.F.R. Part 740, Supplement No. 1. Unsurprisingly, ACE does not authorize exports to embargoed destinations – Cuba, Iran, North Korea, and Syria.

[5] See 81 Fed. Reg. 35586, 6 June 2016.

Reprinted with permission from the May 2023 issue of Export Compliance Manager.
www.exportcompliancemanager.com

government end-users in Country Group D.[4] Further, license exception ACE is unavailable when an exporter knows or has reason to know that the cybersecurity item "will be used to affect the confidentiality, integrity, or availability of information or information systems" without authorization. Due to the sensitivity of the export of cybersecurity items, any party considering using the ACE exception or providing cybersecurity hardware, software, or technology to a foreign person should carefully review the applicable controls and apply appropriate risk-based due diligence to evaluate the end-user and end-use.

Reducing exfiltration risks

Government contractors present an especially attractive target for cyberattacks because their networks often contain critical defense technical data, which is controlled under the International Traffic in Arms ("ITAR") regulations, or military-related technology controlled under the 600 series of the Export Administration Regulations ("EAR"). To minimize the potential damage and liability caused by a cyberattack, government contractors should ensure any export-controlled data is maintained securely on their network (i.e, encrypted, marked, and segregated) and implement systematic data minimizations procedures – the less data on the network, the less information that can be stolen and used to commit cybercrime.

You've been hacked – disclosure requirements and liability risks

If your network is hacked by foreign persons and the cyber actors exfiltrate defense technical data or controlled technology, that "release" of technology or technical data does not constitute an illegal export for which your organization could be held criminally liable because it was done without your authorization. In other words, it was not a knowing or willful violation of the export laws. Nevertheless, at least under the ITAR, such a release may still qualify as a controlled event if the data was in unencrypted form. Thus, your organization should consider making a voluntary self-disclosure to the Directorate of Defense Trade Controls ("DDTC"). In contrast, the EAR codified a safe harbor for hacking victims.[5] Under 15 C.F.R. §734.15(b), the hacker is the one who causes the release of technology and is responsible for the theft rather than the person who placed the technology on the network.

Cyberattacks could give rise to contractual obligations as well as civil liability and criminal liability. Defense contractors are required to comply with cybersecurity standards set forth in Defense Federal Acquisition Regulation Supplement ("DFARS") § 252.204-7012 ("Section 7012"). Section 7012 requires that defense contractors, as well as their subcontractors through flow-down contractual provisions, "rapidly report" cyber incidents to DOD within 72 hours of their discovery. Further, the Biden Administration's new National Cybersecurity Strategy, released in March 2023, indicates that any business operating in the broadly defined "critical infrastructure" sector will soon be required to report cyber incidents "within hours" of their discovery. In October 2021, DOJ announced the Civil Cyber-Fraud Initiative and its intent to use the False Claims Act to hold organizations accountable for cybersecurity noncompliance, including failing to report data breaches. Similarly, the Federal Trade Commission ("FTC") has brought actions against businesses for lax data security and sharing sensitive consumer data with third parties for advertising purposes. Lastly, every state has enacted their own data breach notification laws and numerous states have even adopted comprehensive data privacy laws. Failure to comply with applicable data security and privacy laws may lead to multi-million dollar fines, class action lawsuits, and state or federal enforcement actions.

> Victims of ransomware and extortionware risk violating US sanctions by making payments to cybercriminals.

So what can you do to protect your organization from liability?

Steps to avoid criminal and civil liability

1. Properly safeguard data

Regardless of whether you data is stored locally or in the cloud, you should take steps to secure it using firewalls, encryption, multi-factor authentication, and extended detection and response tools (technology that monitors and mitigates cybersecurity threats to your organization's data across your entire network, cloud, endpoints, and applications).

2. Establish a Cyber Incident Response Plan ("CIRP")

The first 48 hours after discovering that cyberactors have infiltrated your network are critical to securing your network, minimizing the damage, obtaining and preserving evidence, and complying with both contractual obligations as well as legal obligations. Organizations that have a CIRP, have instituted comprehensive cybersecurity training, conduct table-top exercises of their CIRP, and employ detection and response security tools greatly reduce and minimize the damages resulting from cyberattacks or negligent cybersecurity incidents caused by corporate insiders or vendors. Implementing a CIRP also ensures that organizations can meet the stringent and increasing reporting requirements for cybersecurity incidents.

3. Be wary of making ransom payments to hackers

Victims of ransomware and extortionware

risk violating US sanctions by making payments to cybercriminals. It is illegal for any US person to send money to anyone located in an embargoed location or on the Specially Designated National and Blocked Persons ("SDN") List. The Department of Treasury's Office of Foreign Assets Control ("OFAC") has added numerous persons and entities responsible for cyberattacks or cyber espionage to its list of sanctioned malicious cyber actors. OFAC also has designated cryptocurrency wallets used for ransomware activities. Accordingly, companies should be wary of making any payments to a ransomware or hacking group. Failure to conduct thorough due diligence and screening prior to making a ransomware payment could result in both criminal and civil penalties. Sanctions violations carry a maximum of 20 years' imprisonment. OFAC may also impose stiff civil penalties for sanctions violations based upon strict liability.

4. Don't conceal a data breach or engage in obstructive conduct

The recently concluded prosecution of Joseph Sullivan, Uber's former Chief Security Officer, highlights the risks of concealing a data breach and obstructing a federal agency's investigation related to a cyberattack. This was the first time that any corporate officer had been criminally charged or convicted for conduct related to the handling of a data breach. Although this case is atypical, in that Uber suffered a second cyberattack while being investigated for a prior data breach, it should serve as a warning that DOJ will be seeking jail time for corporate insiders who choose to cover up embarrassing cybersecurity mistakes and lie to federal officials. There may be a large pool of potential DOJ targets based upon the Bitdefender 2023 Cybersecurity Assessment. That report found that 71% of cybersecurity teams in the United States "have been told to keep a security breach confidential when it should have been reported." This decision may lead to significant criminal and civil liability, especially if your employees decide to become whistleblowers.

Your employees are likely your weakest link. Implement email geographic restrictions.

5. Use cyber tools to demonstrate compliance and minimize insider threat risks.

Your employees are likely your weakest link. Implement email geographic restrictions. This will prevent phishing emails while also limiting the potential of illegal exports of technology. Block the ability of employees to connect flash drives to your network. Additionally, establish a robust and effective compliance program to identify and prevent potential violations of export laws and sanctions. Due to the advancement in cyber tools, organizations should use automation in their compliance programs to prevent violations of US export laws and sanctions. For instance, OFAC has repeatedly criticized organizations for their failure to incorporate geolocation blocking tools into their screening and business practices. ■

About the author:

B. Stephanie Siegmann is a Partner at the law firm of Hinckley, Allen & Snyder LLP, and Chair of its International Trade and Global Security Practice.

www.hinckleyallen.com

Reprinted with permission from the May 2023 issue of Export Compliance Manager.
www.exportcompliancemanager.com