ARTICLES

PUBLISHED: NOVEMBER 6, 2024

Legal Insights for Manufacturing: Cybersecurity

Service

Data Privacy & Cybersecurity

Industry

Manufacturing

Professional

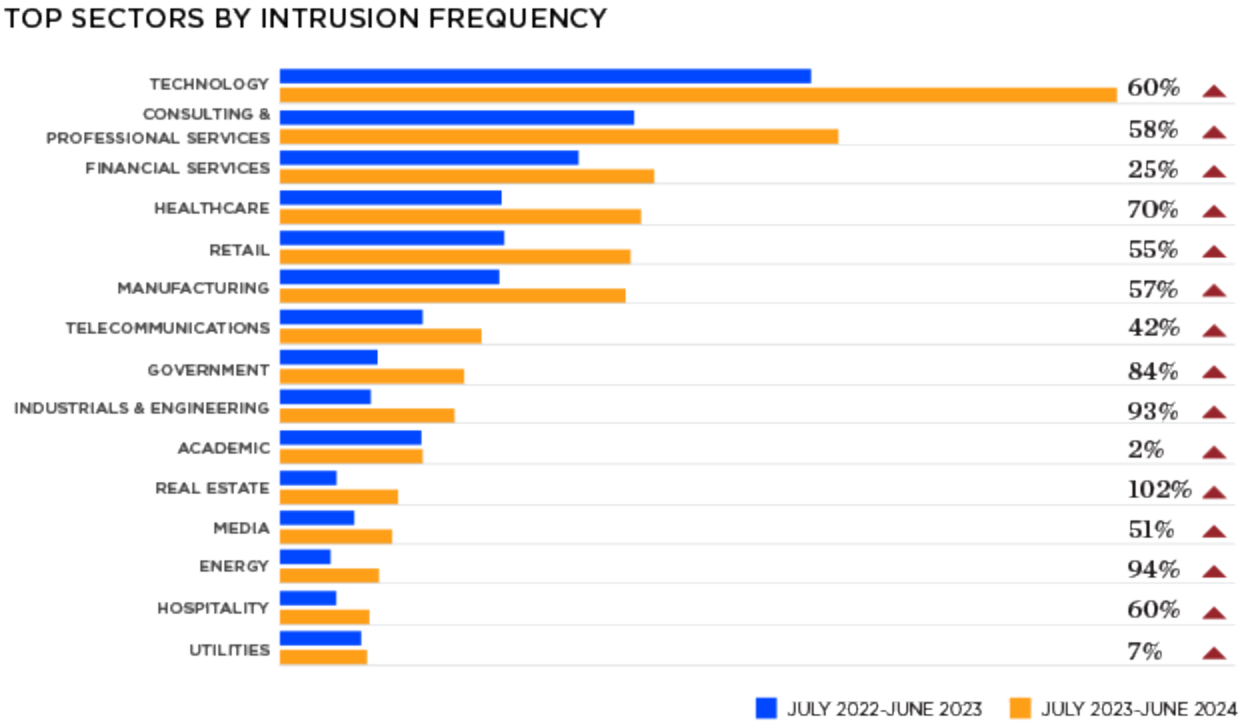
ERIK DULLEA
DENVER:
303.749.7270
ERIK.DULLEA@
HUSCHBLACKWELL.COM

This article is excerpted from our third-annual *Legal Insights for Manufacturing* report, published in October 2024.

Cybercrime continues to be a booming market for criminals— and a growing challenge for information security professionals. According to an April 2024 report by the Congressional Research Service, cybercrime cost the United States an estimated $220 billion in 2022 and $320 billion in 2023. The expected costs in 2024 are $452 billion and are forecasted to exceed $1 trillion in 2027.

Cybersecurity, Manufacturing & Its Enabling Technologies

Consistent with last year's statistical trends, manufacturing remains a frequently targeted sector for malicious cyber activities. According to CrowdStrike, a cybersecurity company and provider of endpoint security services, the industry experienced a 57 percent increase in cyber intrusions compared to the prior year, but what is equally concerning is the prevalence of attacks against the technology sector, which includes developers of software and hardware, information technology (IT), and IT service providers. These businesses are relied upon by every other industry sector—including manufacturing; therefore, the growing cybersecurity challenge for tech companies creates significant third-party risk.



Source: *CrowdStrike 2024 Threat Hunting Report.*

Ironically, CrowdStrike provided a glaring case study on the ripple effects caused by a disruption within a technology services company. On July 19, 2024, the company was the source of a flawed software update deployed worldwide to Microsoft Windows servers, causing the "blue screen of death" across 8.5 million computers worldwide. Fortunately, the flaw was due to benign human error, not a malicious actor who sought to evade detection. Nevertheless, downstream consequences from a simple coding error in a software update illustrates both the liability risks manufacturers face when they place their electronic components into the marketplace, as well as the business interruption risk they face when receiving new components from their suppliers. Both require the attention of compliance, legal, and/or contracting teams to have plans in place in the event of a mishap.

CISA's Proposed Rules for Cyber Incident Reporting for Critical Infrastructure

In March 2024 the Cybersecurity and Infrastructure Security Agency (CISA) released a Notice of Proposed Rulemaking (NPRM) to implement regulations mandated by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The proposed regulations echo Congress's statutory deadlines for large critical infrastructure companies to report substantial cyber incidents to CISA within 72 hours. Additionally, the law requires covered entities to report ransom payments to CISA within 24 hours of the payment being made.

While CIRCIA set forth these reporting timeframes, the statute did not expressly define covered entities or covered cyber incidents. The proposed regulations provide definitions for those terms. CISA's proposed definition for covered entities would be owners and operators of critical infrastructure that exceed the small business size standard associated with the owner/operator's North American Industry Classification Standard, or NAICS, code. CISA's proposed definition for a covered cyber incident would be a substantial cyber incident experienced by a covered entity.

Pursuant to the Patriot Act and two presidential directives, U.S. critical infrastructure is defined as those industry sectors with vital assets, systems, and networks (physical or virtual) such that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The Department of Homeland Security designated 16 industry sectors as critical infrastructure, each of which has an assigned Sector Risk Management Agency (SRMA) that is charged with providing resources and coordination to assist industry participants in the event of an incident.

CISA's proposed rule provides the agency's methodology for determining when a cyber incident is elevated to the category of *substantial cyber incident*, which is defined as an incident that leads to one of the following impacts:

Substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;

Serious impact on the safety and resilience of a covered entity's operational systems and processes;

Disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services; or

Unauthorized access to a covered entity's information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either (1) a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (2) a supply chain compromise.

The proposed definition of a substantial cyber incident would require one or more actual impacts to occur. An attempt to cause a loss of confidentiality or disrupt a covered entity's ability engage in business would not be reportable because there was no impact.

SEC Cybersecurity Rule Developments

One concern that private industry has expressed with the increased cyber reporting requirements is that the information will be used by other enforcement agencies to punish the victim company. While

there is always a risk of dubious enforcement actions in the absence of safe harbor provisions within reporting laws, the SEC's efforts to become a cybersecurity enforcement agency—discussed at length in last year's report—hit a roadblock this summer in the SEC's case against SolarWinds.

DESIGNATED SRMA BY INDUSTRY SECTOR

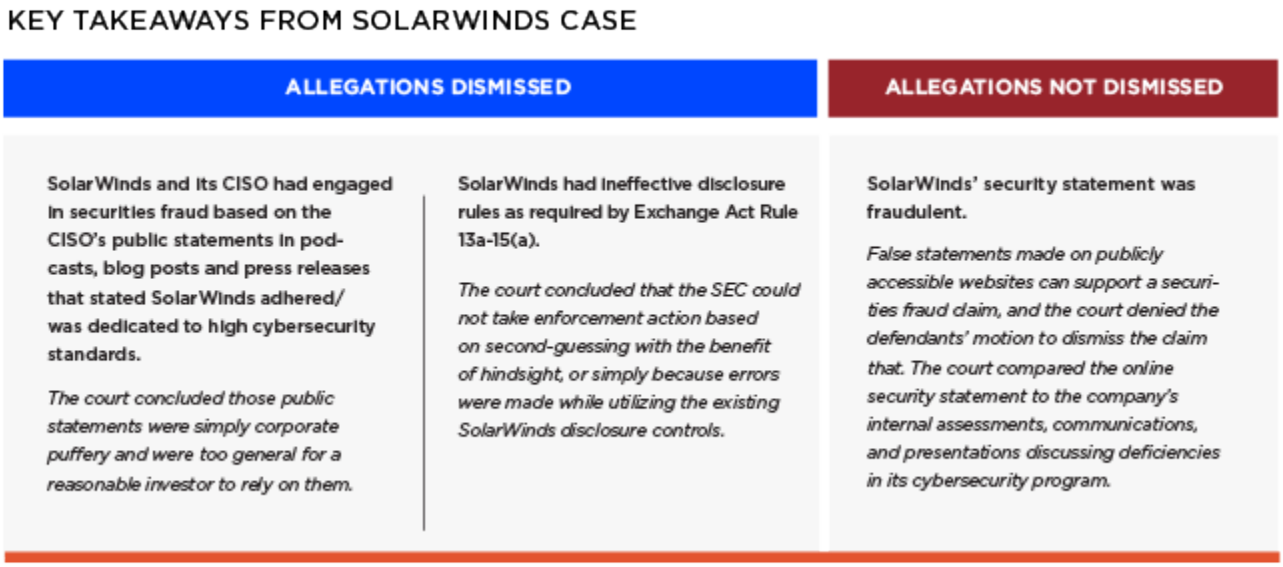
Sector	DHS	DOD	DOE	DOT	EPA	GSA	HHS	TREAS	USDA
CHEMICAL	•								
COMMERCIAL FACILITIES	•								
COMMUNICATIONS	•								
CRITICAL MANUFACTURING	•								
DAMS	•								
DEFENSE INDUSTRIAL BASE		•							
EMERGENCY SERVICES	•								
ENERGY			•						
FINANCIAL SERVICES								•	
FOOD AND AGRICULTURE							•		•
GOVERNMENT FACILITIES	•					•			
HEALTHCARE/PUBLIC HEALTH							•		
INFORMATION TECHNOLOGY	•								
NUCLEAR	•								
TRANSPORTATION SYSTEMS	•			•					
WATER/WASTEWATER					•				

Source: Presidential Policy Directive—Critical Infrastructure Security and Resilience, February 12, 2013.

On October 30, 2023, the SEC filed a complaint against SolarWinds, a software development company, and its chief information security officer (CISO). The complaint caused significant concern among the information security community because the SEC alleged that between the date SolarWinds became a publicly traded company (2018) and January 2021, SolarWinds made materially misleading statements and omissions in public disclosures and statements regarding the company's cybersecurity practices. The SEC argued these statements caused a significant drop in the

company's stock price after the December 2020 disclosure of a large-scale cybersecurity attack known as SUNBURST.

The statements that the SEC took issue with included the company's periodic filings that only described generic and hypothetical cybersecurity risks but failed to specify cybersecurity risks that were known to the company. The SEC argued that the SolarWinds online security statement claimed that the company followed cybersecurity standards like the National Institute of Standards and Technology Cybersecurity Framework, utilized strong authentication and password policies, and maintained adequate access controls when those practices were not followed. The SEC also alleged the company and CISO of concealing deficient cybersecurity controls and identified vulnerabilities that left its systems susceptible to attack, which were highlighted by internal company records voicing concerns with the deficiencies.



Based on those facts, the SEC charged SolarWinds and its CISO with direct anti-fraud violations for alleged misstatements as well as direct and secondary liability against them for internal controls violations. The defendants moved to dismiss the complaint, which the court partially granted on July 18, 2024 (four days before the CrowdStrike patching error disrupted the world's economy for a few hours). The court's decision was significant because it addressed several concerns within the information security community regarding the SEC's enforcement powers over a company's cybersecurity practices.

Notably, the court compared the company's online security statement to its internal assessments, communications and presentations discussing deficiencies in its cybersecurity program. These

internal assessments and communications are vital to a company's ability to identify, prioritize and assess its cybersecurity risks, and those communications should not be stifled.

However, corporate leaders must acknowledge that such assessments and communications can be used in enforcement actions if they are apposite to the company's official statements to customers and investors about its security controls. Accordingly, publicly traded companies— and those aspiring to be publicly traded or acquired—must strive to be consistent between their cybersecurity assessments and their public statements on cybersecurity.