wiley

NEWSLETTER

2022 Cyber Watch List: A look at 2021 and What's to Come in the Year Ahead

January 2022

Privacy In Focus®

In 2021, cyber gained prominence as a top business risk and national security concern with ransomware attacks wreaking havoc on business operations and critical infrastructure.[i] Companies large and small, as well as state or local governments, were forced to make the difficult choice between making a ransom payment to threat actors or risking significant operational disruptions, loss of data or revenue, and reputational injury. The volume of ransomware attacks and the size of the demands simply skyrocketed in 2021.

Look what happened in the summer of 2021 alone: In May, Colonial Pipeline paid a $4.4 million ransom after an attack compromised its operations and caused gas shortages throughout the East Coast.[ii] In June, JBS paid $11 million ransom after an attack caused the company to close its meat processing plants causing meat prices to soar.[iii] In July, Kaseya, an information technology software provider, received a $70 million ransom demand to unlock millions of infected systems.[iv] Some of the most pressing cyber-enabled threats confronting the nation in 2021 involved attacks that resulted in serious shortages affecting millions of consumers or insidious supply chain malware attacks emphasizing how interconnected, and how vulnerable, all our computer or information systems have become.

What will we see in 2022? Here are the top 5 cyber issues to watch for in the coming year:

1. The Race to Cyber Incident Reporting

Authors

Jacqueline F. "Lyn" Brown
Of Counsel
202.719.4114
jfbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

Transactional Support and Due Diligence on Privacy and Cybersecurity

As the number of high-profile ransomware attacks gained public attention, 2021 saw numerous attempts to pass some sort of mandatory cyber incident reporting. While the U.S. House of Representatives passed legislation requiring companies to send reports to the Cybersecurity and Infrastructure Security Agency (CISA) 72 hours after an incident, the measure was pulled out of the National Defense Authorization Act (NDAA) at the last minute. The need for such legislation seems obvious enough. Both CISA and the U.S. Department of Justice (DOJ) favored mandatory cyber incident reporting to give the government a more complete view of the cyber threat environment and the risks to our national and economic security. Without a legal reporting requirement, the Federal Bureau of Investigation (FBI) was left to strongly urge victim companies to report ransomware incidents while it discouraged them from actually paying the ransom demand.

But an odd thing happened on the way to the Hill. The FBI, as the agency principally responsible for investigating cybercrime, was left out of the reporting notification provisions in favor of CISA. To its credit, CISA said it would share cyber incident reports with the FBI regardless of what type of legislation Congress passes. Still, 2021 ended with the spectacle of the FBI having to raise its hand to Congress and say "me too" for cyber incident reporting and getting rebuked which was a tough way to end the year. Look for DOJ and FBI to continue to press the case for cyber incident reporting to the FBI, frequently with private sector support, as Congress takes up this important issue in 2022.

2. The Rush to Regulate Cyber Standards and Punish Cybersecurity Deficiencies

As cyber threats continued to dominate the news, federal departments and agencies increasingly started to flex their regulatory muscles in 2021. In September 2021, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities. [v] OFAC advised that companies that facilitate ransomware payments to cyber actors on behalf of victims (including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response) encourage future ransomware payment demands and risk violating OFAC regulations. [vi] Because the U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands, Treasury recommended focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks. [vii] For 2022, look for more action by Treasury on financial transparency regarding virtual assets as the government tries to address the abuse of virtual currency to launder ransom payments.

DOJ also sent a strong signal in 2021 about increasing corporate enforcement mechanisms to change corporate behavior so that effective cybersecurity compliance programs are put in place. DOJ launched a civil cyber fraud initiative to combat new and emerging cyber threats to critical and sensitive information systems. DOJ essentially put companies on notice that it will not hesitate to use its civil enforcement authorities to pursue government contractors under the False Claims Act when they fail to follow required cybersecurity standards. In light of these DOJ initiatives, for 2022 companies should consider their cybersecurity, privacy, and supply chain programs. Companies can help protect against civil fraud enforcement and other litigation and oversight by reviewing relevant cybersecurity requirements and incorporating government guidance into their own risk management plans.

The Biden Administration has made it clear that the private sector, which owns and operates the majority of U.S. critical infrastructure, must do more to modernize their cyber defenses to meet the threat from ransomware.[viii] For 2022, the government will continue to try to improve the cybersecurity posture of the private sector through a variety of regulatory requirements or proposed enforcement actions. Look for the government to expand regulatory obligations, oversight, and accountability for private sector entities at risk from cyber-attacks, particularly those in critical infrastructure.

3. More Ransomware Attacks But FBI Shifts Focus to Victim Assistance and Asset Recovery

One of the highlights of 2021 in the fight against cyber crime was the seizure of ransom proceeds from the virtual currency wallets of malicious cyber actors. A month after the ransomware attack against Colonial Pipeline, the FBI successfully seized $2.3 million from a bitcoin wallet that ransomware actors had used to collect the cyber ransom payment. [ix] The Colonial Pipeline seizure of ransom payments was just the beginning. Shortly after the government successfully seized $2.3 million from ransomware extortionists, DOJ announced that the government had recovered $6.1 million in ransom payments made by Kaseya, a multi-national information technology software company, after its systems were attacked by Sodinokibi/REvil ransomware in July 2021.[x] The government was also able to obtain decryption keys and provide the keys to the managed service provider whose systems had been victimized.

Despite government success in retrieving some ransomware proceeds, 2021 showed how lucrative ransomware attacks could be for malicious cyber actors. Look for an increase in "double extortion" ransomware where the bad actors encrypt, steal, and then threaten to leak or sell the victims' data in 2022.[xi] Double extortion raises the stakes considerably for victims and increases the chances that they will decide to make the ransom payment. [xii] This is likely to emerge as a leading tactic for cybercriminals.[xiii]

For 2022, look for the government to combat ransomware attacks by depriving the bad actors of monetary gains. "Follow the money" has long been a law enforcement priority well before the phrase was popularized by the Watergate investigation. But look for the government to provide decryption keys if available too. Look for the FBI, in particular, to focus less on traditional indictments and more on asset recovery and incident response.

4. A Federal Standard of Cybersecurity Care Emerges

2021 marks the shift in the government from reacting to cyber crime to attempting to establish a federal standard of cybersecurity care which will only increase in 2022. In July 2021, the Biden Administration issued *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* in response to the high-profile cyber-attacks against critical infrastructure to develop cybersecurity performance goals that are consistent across all critical infrastructure sectors. In this ongoing effort, CISA, in coordination with the National Institute of Standards and Technology (NIST), are creating cybersecurity performance goals for critical infrastructure partners that include applicable objectives and sample evidence of implementation. The "Common Baseline" for improving cybersecurity for critical infrastructure is shaping up to be a "best practices" guide from the government.

Similarly, in November of 2021, CISA released the Federal Government Cybersecurity Incident and Vulnerability Playbooks as part of the Biden Administration's efforts to improve the nation's cybersecurity. The Playbooks are intended to apply to federal civilian executive branch agencies. But, they also apply to federal contractors who operate information systems on behalf of a federal civilian agency; and, information and communications technology (ICT) service providers who have contracts with federal civilian agencies. When releasing the Playbooks, CISA encouraged all public and private sector partners to review them as a way to check their own vulnerability and incident response practices. While the Playbooks may not be binding on the private sector the way they are on the government, federal contractors, or ICT service providers, the private sector should consider how their cybersecurity practices compare to what is in the Playbooks, because the government has made it clear that it expects companies to improve their cybersecurity in response to increased threats from malicious cyber actors. The Playbooks are another signal to the private sector about what the government considers to be the relevant standard of care for cybersecurity.

Look for both the "Common Baseline" (when completed) and the CISA Playbooks to be cited in regulatory or enforcement actions for cybersecurity deficiencies in 2022.

5. Companies Prioritize Cybersecurity

In 2021, companies became more aware of cyber threats as more and more high-profile cyber-attacks made the news and federal departments and agencies became more aggressive in trying to counter cyber threats to our national and economic security. As they grow more reliant on digital technology, companies increasingly store electronically ever larger amounts of data about their business and customers which are attractive targets for cyber criminals to try to steal or compromise. Malicious cyber threat actors have become increasingly sophisticated in how they pick and try to extort their victims.

In 2022, companies need to prioritize cybersecurity to protect against malicious threats to their operations, data, and revenue streams. In doing so, companies can look to federal contracting standards, NIST publications, and now the CISA Playbooks and "Common Baseline" for guidance. The Playbooks have, for instance, a helpful incident response checklist in Appendix B with steps from Detection & Analysis, to Containment, to Post-Incident Activities. The Playbooks may not be binding on the private sector, but they are extremely instructive about what the government believes are the minimum requirements for cybersecurity.

For 2022, companies can also help protect themselves against regulatory review and possible enforcement actions by reviewing the relevant cybersecurity requirements in their sector and making necessary adjustments to comply with the standards the government is setting for itself and establishing as its de facto standard of care. Companies can use the threat information provided by FBI, CISA, and other agencies to strengthen network defenses and guard against ransomware and other malicious cyber activity. Organizations, especially government contractors, should continue to evolve their incident response practices as the government issues more internal standards for the civilian executive branch.

Look for more tension with the government and possibly more confusion about federal standards as we move into 2022. Parts of the government would sincerely like to increase public-private partnership, particularly with those in critical infrastructure. But other relevant federal departments and agencies are increasingly seeking to use their authorities to fight the cyber threat by punishing perceived cybersecurity deficiencies. For 2022, this means increased regulatory requirements to incentivize good cybersecurity and more enforcement actions in the future to penalize what the government perceives to be deficient cybersecurity.

Going forward, there will be substantial growth in regulatory requirements and oversight with new and enhanced disclosure requirements. Federal regulators will increasingly leverage their authorities (and seek new powers) to demand that companies address the threats posed by ransomware, update outdated industrial and operational control systems, address software vulnerabilities, and more. 2022 is shaping up to be the year of cybersecurity standards and compliance.

---

[i] https://www.lawfareblog.com/ransomware-payments-and-law

[ii] https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

[iii] https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

[iv] https://www.wsj.com/articles/kaseya-ransomware-attack-11625593654

[v] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[vi] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[vii] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[viii] https://www.google.com/search?q=fact+sheet%3A+ongoing+public+us+efforts+to+counter+ransomware&rlz=1C1GCEA_enUS975US976&oq=fact+sheet%3A+ongo&aqs=chrome.1.69i57j69i59.6297j0j7&sourceid=chrome&ie=UTF-8

[ix] https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline

[x] https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

[xi] https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf

[xii] https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf

[xiii] https://www.judiciary.senate.gov/imo/media/doc/Vorndran%20-%20Statement.pdf