Government Contracts and Privacy & Cybersecurity Update

March 2022

White House Warns of Imminent Cyberattacks; Describes Threat Mitigation Measures

Key Notes:

- On March 21, 2022, President Biden warned American businesses to prepare for imminent cyberattacks from Russian-backed hackers.
- Organizations should review their information security programs and identify whether they align with an appropriate security standard, especially those organizations identified as critical infrastructure as they face heightened cyber risk.

On March 21, 2022, President Biden issued a statement noting "that the Russian Government is exploring options for potential cyberattacks" against the United States in "response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners" for Russia's actions in Ukraine. Given that most of the critical infrastructure in the United States is owned and operated by the private sector, President Biden called on these sectors to "do their part" to prevent and mitigate cyberattacks by "accelerat[ing] efforts to lock their digital doors."

As part of the warning, the U.S. government issued a related guidance Fact Sheet for organizations to take certain cyber defense actions, and these actions mirror the recommendations previously issued by the federal government. These security actions include the following:

- Mandate multi-factor authentication to make it harder for attackers to access systems.
- Deploy modern information system security scanning tools. Ensure systems are patched and protected against all known vulnerabilities.
- Engage IT consultants to verify the sufficiency of your organization's security controls.
- Update passwords across networks so previously stolen credentials cannot be reused by malicious actors.
- Back up data and ensure they are secure and retrievable.
- Practice security incident tabletop exercises.
- Encrypt data so it cannot be used if stolen.
- Educate staff and employees about security threats and their obligations.
- Establish relationships with the FBI and/or CISA to streamline post-incident engagement.

Organizations that are subject to federal or state data security regulations, such as federal healthcare information security rules and defense contracting regulations governing the protection of Controlled Unclassified Information ("CUI"), should be well aware of these types of security requirements. However, the White House's recommendation addresses information security in more contextual terms and may be helpful guidance for any organization.

Best-Practice Recommendations

In addition to the recommendations set forth by the White House, there are other practices that organizations should consider incorporating into their security programs.

- **Identify and Protect Regulated Data.** Businesses collect data for a number of reasons, including providing services or products to private and public sector customers, marketing those services or products to existing and potential customers, and administering

their internal employees and personnel. In order for such data to be properly safeguarded, organizations need to be able to identify, in accordance with a risk-based criteria, the types of data they retain, where it is stored, how it is accessed and shared, and the timeframe and mechanisms used to dispose of it at the end of its lifecycle. Accordingly, organizations should undertake detailed data inventory and mapping exercises to identify all sensitive or otherwise regulated data within an organization's custody and control, including personal data and CUI.

- **Cyber Risk Insurance.** A key part of any cyber risk mitigation plan is cyber or data protection insurance, which can minimize loss and damages following a ransomware attack or other cybersecurity event. Accordingly, organizations must understand the scope of their insurance coverage, potential exclusions (such as wartime or hostility exclusions), and claims notification timelines and processes. In the event such insurance is not adequate, organizations should immediately seek to identify whether they can procure supplemental or replacement coverage to minimize the risk. It is also important for organizations to understand whether their insurance carrier requires them to retain insurance-approved security consultants or law firms following an incident, and ensuring these outside stakeholders are incorporated into the organization's incident response plan.
- **Establish a Clear Vendor Security Management Program and Policy.** An organization's information security program is only as strong and sufficient as the third parties that process and retain their data. In turn, a vendor security management policy or program validates whether a third-party service provider can implement and maintain an information security program that complies with all applicable laws, statutes, and regulations, and data protection standards set forth by a business. Organizations should ensure their service provider contracts include appropriate data protection clauses based on the scope of the services and risk levels, such as specified security standards, confidentiality rules, and data localization requirements. These requirements should be supported by information security policies, security attestation, and audits, which the service provider should furnish to your organization on an ongoing basis. In order to minimize loss in this area, service provider contracts should include clear rules and responsibilities in the event of data breach, including any notification and indemnification obligations. It is also important that these standards and criteria are included in any subcontractor terms and conditions. Organizations should consider such a vendor management program even if they are not subject to federal or state laws that mandate similar requirements.
- **Closely Monitor Cybersecurity Resources to Track New Threats as They Appear.** Organizations should monitor any security updates and warnings regarding cyber threats. With the potential rollout of new malware by Russia or other state-sponsored actors, organizations must stay abreast to evolving cyber threats and be prepared to implement any mitigating security patches or programs. The U.S. Department of Homeland Security, the Federal Bureau of Investigation, and other federal agencies routinely publish cyber threat alerts and should be a resource for any organization.

Conclusion

It is imperative that organizations operating in, or supporting, critical infrastructure sectors understand and respond to current cybersecurity threats arising from the Russia-Ukraine war. If your business needs assistance in developing or updating an information security program, please contact one of our Thompson Hine attorneys below.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com

Mona Adabi
202.263.4147
Mona.Adabi@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com