Shields Up: Russian Cyberattacks Headed Our Way

May 4, 2022

Russian Cyberattacks

As we watch the televised Russian invasion of Ukraine with horrific destruction and casualties caused by missiles, tanks, and other conventional warfare the hostilities may seem far away and distant. As Russia continues to suffer setbacks in their conventional military approach we are likely to see cyberattacks that could spread beyond the Russian-Ukrainian conflict.

The FBI has warned businesses, banks and local governments about this increased risk of cyberattacks, and the Cybersecurity & Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security has issued a "Shields Up" warning to counter possible Russian attacks. President Biden recently told U.S. business leaders, "We need everyone to do their part to meet one of the defining threats of our time — your vigilance and urgency today can prevent or mitigate attacks tomorrow."

In addition to buttressing technical cyber defenses, businesses need to check their risk management approach, review cyber insurance policies for "act of war" exclusions, and make sure they have adequate coverage for ransomware and other cyber-attacks. Now is the time for all businesses, regardless of size, to review their incident response programs, conduct gap analyses and engage in practice "table-top" exercises before an actual data incident occurs. While there is no need to panic, all businesses, regardless of size, should review their data security program and practices to make sure they are ready for any cyber-attack.

Safeguards Rule of the Gramm Leach Bliley Act

If the prospect of a Russian cyberattack does not motivate a business to update its data security practices, the possibility of an enforcement action from regulators like the Federal Trade Commission (FTC) should.

On October 27, 2021, the FTC announced the final amendments to the Safeguards Rule of the Gramm Leach Bliley Act, expanding the definition of "financial institutions" covered by the law. Further the amended rule imposes new and burdensome data security requirements. Although not effective until October 27, 2022, affected businesses should already be taking steps to comply.

For example, higher education institutions and motor vehicle dealers are just two non-banking "financial institutions" that fit an expanded definition of so-called "finders" who must now implement and maintain a

comprehensive data security system that protects customer information.

The amended Safeguards Rule imposes a wide array of data security requirements, including encryption, employee training, secure development practices, MFA, information disposal procedures, vendor management, regular reporting to boards of directors, and assigning a manager to oversee the data security program. A business that complies with the new Safeguards Rule will enjoy the further benefit of stronger defenses against cyberattacks from Russia or elsewhere.

Companies must continue to do the basic blocking and tackling: upgrade and test backups, implement multi-factor authentication (MFA), and patch vulnerabilities. To those businesses who have yet to experience ransomware, cyberattacks, data breach, or other forms of unauthorized access to data, it remains a matter of when, not if, such events will occur.

Our Global Privacy, Cybersecurity & Data Protection Group can assist with the preparation of Written Information Security Programs, Written Incident Response Plans, and serve as counsel in the event of a data breach, including ransomware, cyber-attacks, or other unauthorized access to or use of protected data.