Articles + Publications | June 23, 2021

Updating Your "Reasonable Security" During the "Ransomware Outbreak"

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

"Reasonable Security" is a term that is becoming more important due to the continued increase in ransomware incidents over the past few years, which the U.S. Cybersecurity and Infrastructure Security Agency ("CISA") has described as the "ransomware outbreak." Responding to this increased threat environment, the Center for Internet Security (CIS) has updated its previously issued CIS 20 Controls to the CIS 18. This set of Controls is among a few examples of security controls that have been specifically suggested by the California Attorney General's Office as meeting a "minimum level of information security that all organizations that collect or maintain personal information should meet." While the CIS Controls can help meet the minimum level of information security, many organizations will be held to a higher standard, because the data they process and maintain require more than just the minimum level of information security. For a robust information security program that can adapt to your organization's changing needs, existing state cybersecurity requirements offer a promising alternative.

When looking to state laws for guidance on reasonable security, some state laws apply generally and some are specific to sectors of the economy. The Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00, is an (actually, the first) example of a state requirement of general applicability. This regulation requires organizations that own or license Massachusetts residents' personal information to maintain a written, comprehensive information security program ("WISP") addressing specific security risks and to meet certain requirements such as the encryption of personal information.

An example of state sectoral laws is the NAIC Insurance Data Security Model Law, which requires entities regulated by the insurance departments in the various states that have adopted the model to meet specific information security and reporting requirements tailored to the insurance industry. These laws complement the major federal sectoral privacy laws, HIPAA and GLBA, which have their own security requirements. While these sectoral laws provide some helpful guidance, they are rarely flexible enough to apply well outside of the sector that they were designed to serve.

A valuable framework for reasonable security should be both comprehensive and flexible. The New York Department of Financial Services Cybersecurity Regulation (NYDFS CR) is a framework that is flexible enough to help organizations of any size and focus to secure their information systems, as recognized by the FTC's adoption of its provisions into proposed amendments to the GLBA Safeguards rule. While every organization is different, the NYDFS CR bases organizational security on its requirement of a periodic risk assessment. The periodic risk assessment forms the baseline for implementing and drafting the WISP, managing third party vendors, training employees, encrypting data, and arranging all other aspects of a healthy cybersecurity program. Many organizations today may not fit the older frameworks, which were designed for governments, defense

contractors, and other large companies. Modern startups are often processing sensitive data in the context of heavy reliance on third party vendors or web platforms as their information systems. NYDFS CR incorporates these scenarios because it was designed to apply across the spectrum, from solo insurance agents all the way to large financial institutions. As such, NYDFS CR can be used as guidance for any organization looking for a way to assess and adapt its cybersecurity program to modern risks in a way that is both protective and cost sensitive. However your organization is adjusting to the ransomware outbreak, it may be helpful to take a look at NYDFS CR for practical ways to improve the security and resilience of your information systems.

---

[1] California Data Breach Report 2016, California Attorney General (February 2016), at p. 10, available at: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

[2] 201 CMR 17.00, available at https://www.mass.gov/doc/standards-for-the-protection-of-personal-information-of-ma-residents-201-cmr-1700/download.

[3] 23 NYCRR Part 500

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber