HINSHAW

The Illinois Department of Insurance Issues Cybersecurity Guidance Regarding Microsoft Exchange Server Installations

Privacy, Cyber & AI Decoded Alert | 2 min read
Jun 4, 2021

The Illinois Department of Insurance (the "Department") recently released guidance to all regulated entities concerning vulnerabilities in Microsoft's Exchange Server installations. Issued on the heels of other state and federal agency warnings and directives, the guidance outlines pertinent details of the vulnerabilities and what successful exploitation of these vulnerabilities could mean—namely "persistent system access and control of an enterprise network." Recognizing that servers may still be compromised even after March and April fixes have been applied, the Department urges regulated entities to:

- Immediately assess the risk to their systems and consumers and take steps to address them;
- Identify internal use of vulnerable Microsoft Exchange products and any use of these products by critical third parties;
- Immediately patch or disconnect vulnerable servers and use tools provided by Microsoft to identify and remediate; and
- Continue to track developments and respond quickly to new information.

Although failure to follow the Department's guidance cannot result in an enforcement action at this juncture, it could potentially support claims in a civil or criminal action given the overwhelming amount of public notice.

Also significant is that the guidance is yet another example of a government agency seeking to monitor and advise on cybersecurity events. This further demonstrates increased governmental interest and foreshadows potential legislation in Illinois and at the federal level. Businesses that already have risk assessment tools and cybersecurity policies in place will be in an excellent position to meet and comply with any future requirements. In addition, it is noteworthy that the average cost of a data breach in 2020—according to the Ponemon Institute—was 3.86 million dollars, which in the short term can significantly impact an organization's operations. Given the

possible risks of such a serious and large scale event, we strongly advise businesses to follow the Department's guidance.

Related Content

- Iowa Becomes the Latest State to Adopt the NAIC Model Cybersecurity Law
- New NYS DFS Cyber Insurance Risk Framework Warns Against Ransom Payments, Includes Notice to Law Enforcement Policy Requirement
- Connecticut Insurance Department Issues Guidance on Cyber Law Set to go Into Effect

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Insurance