Illinois requires state employees to receive cybersecurity training

Christine N. Czuprynski | Monday, August 28, 2017

On Monday, August 7, Illinois' Gov. Bruce Rauner signed Section 25 of the Illinois Data Security on State Computers Act, which requires Illinois state employees to receive annual cybersecurity training. The training is meant to help state employees detect and avoid phishing scams, prevent spyware infections, and learn how to prevent and respond to data security breaches. Phishing emails trick recipients into giving up personal information that is then exploited for financial or other gain. Phishing emails directed at corporate employees or state agency staffers often trick those individuals into providing their log-in credentials, which are then used to access the enterprise and all of its systems. Avoiding phishing scams will go a long way in the fight against cyber criminals; a report issued by Phish Me at the end of 2016 concluded that 91% of cyberattacks are the result of a spear-phishing email campaign.

The Illinois Department of Innovation and Technology plans to adopt rules to implement the requirements of Section 25, which is effective Jan. 1, 2018. This law is the latest part of a statewide cybersecurity push announced by the Rauner administration in March 2017. The State of Illinois Cybersecurity Strategy focuses on five strategic goals:

1. Protect State of Illinois Information & Systems
2. Reduce Cyber Risk
3. Best-in-Class Cybersecurity Capabilities
4. Enterprise Approach to Cybersecurity
5. A Cyber-Secure Illinois

Section 25 exempts some state workers, including staffers in the legislative and judicial branches,

constitutional officers except the Governor himself, and employees of public state universities. At the bill's signing, the Governor's office reported that most employees for whom this bill applies have already received their training. Most states offer cybersecurity training for state employees, but do not mandate such training by statute. Illinois now joins 14 other states that require some level of cybersecurity training for new employees, for existing employees on an annual basis, or both:

1. Colorado
2. Florida
3. Louisiana
4. Maryland
5. Montana
6. Nebraska
7. New Hampshire
8. North Carolina
9. Ohio
10. Oregon
11. Pennsylvania
12. Utah
13. Vermont
14. Virginia

Private businesses should take this cue from the states and examine their internal policies and procedures related to cybersecurity. New hire and annual training should be a part of any company's cybersecurity policy. There is no excuse for leaving employees – those people who are on the front lines of the cybersecurity war – ill-equipped for the task at hand.

Christine N. Czuprynski

Team member bio