BusinessManagement DAILY

FEBRUARY 23, 2022

The DOL makes 401(K) cybersecurity recommendations

Last year, the Department of Labor released a trio of documents advising employers with 401(k) plans about cybersecurity. The DOL is backing up the advice in those documents during plan audits by scrutinizing employers' and third parties' cybersecurity efforts.

Perhaps the DOL should secure its own computer systems first. A newly released report by the DOL Inspector General concludes the agency's cybersecurity efforts have improved, but not enough. The investigation was conducted by the accounting firm KPMG.

How the DOL thinks about cybersecurity

It's useful to think about cybersecurity the way the federal government does. It has a framework for assessing the effectiveness of federal agencies' cybersecurity efforts. This framework is easily translatable to your business and will help you communicate with IT.

There are five cybersecurity framework functions, which are paired with eight metric domains:

- **Identify:** Identify and maintain an inventory of hardware and software to aid in the development of an understanding on how to manage cybersecurity risks to systems, assets, data and capabilities. *Metric domain:* Risk management.
- **Protect:** Ensure critical infrastructure services are delivered by developing and implementing safeguards. *Metric domains:* Configuration management, identity and access management, data protection and privacy and security training.
- **Detect:** Develop and implement activities to identify a cybersecurity event. *Metric domain:* Information security continuous monitoring.
- **Respond:** Develop and implement actions regarding a detected cybersecurity event. *Metric domain:* Incident response.
- **Recover:** Develop and implement activities to maintain systems' resilience and to restore services impaired due to a cyberattack. *Metric domain:* Contingency planning.

The response levels range from 1 (*ad hoc*) to 5 (optimized). Level 4—Managed and Measurable—is the minimal acceptable standard. To meet this standard, the DOL is required to use metrics to measure and manage the implementation of its cybersecurity programs, control ongoing risks and to perform ongoing system authorizations.

Office of the Inspector General: The DOL met level 4 standards in only two functions: protect and respond. Three areas of metric domains—configuration management, identify and access management and data protection and privacy—achieved only a level 3 rating (i.e., consistently implemented).

Recommendations

The OIG's basic recommendation to DOL is training, training and more training. In other words, employees can't ever be trained enough. This isn’t bad advice for you, either. For example, the OIG suggested training in the following areas:

- Employees should be trained on how to address operational activities.
- The chief information officer should train managers on how to remove access to systems for separated employees. Terminated employees who maintain access to the company’s computer networks can steal confidential information and generally cause havoc.
- The CIO should train employees who oversee cloud operations on how to use third-party continuous monitoring review checklists. This ensures third-party providers operate in a manner consistent with the DOL’s requirements.

Good cybersecurity also entails knowing where your computers are at all times. Remember all those laptops you handed out two years ago? Have you kept track of who got what computer and which software was loaded onto those computers? Admittedly, it’s a Herculean task. Well, according to the OIG, the DOL hasn’t finished implementing a system to track hardware and software devices connected to its networks on a near real-time basis, either.

The OIG also suggested the DOL provide additional resources to support operational activities during unforeseen circumstances and to update the patching process to ensure patches are applied expeditiously.