FEATURE

Ensuring That Cybersecurity Is Everyone's Job

Employees focus on the responsibilities that are listed in their job descriptions. If cybersecurity and privacy responsibilities are not documented in job descriptions, then it is likely that staff members will assume that cybersecurity is not a primary responsibility for them because management did not consider it significant enough to include. The implication is that it is someone else's job. This is a problem because cybersecurity introduces some of the most significant risk scenarios facing enterprises today. To respond to these risk scenarios, the entire staff of an organization must pay attention to cybersecurity. Neglecting to inform staff of their specific responsibilities for security and privacy is a grave oversight.

Published in September 2020, Revision 5 of the US National Institute of Standards and Technology (NIST) Special Publication (SP) SP 800-53 *Security and Privacy Controls for Information Systems and Organizations* contains many valuable changes compared to earlier versions. One significant change is the addition of control PS-9, Position Descriptions.[1] The control description is only 11 words: "Incorporate security and privacy roles and responsibilities into organizational position descriptions."[2] However, in NIST SP 800-53B *Control Baselines for Information Systems and Organizations*,[3] which NIST uses to identify the controls to group into low-, moderate- and high-impact security control baselines, NIST emphasizes the importance of this new control by including PS-9 in each of the baselines. Therefore, any organization using SP 800-53 as its control framework should be including security and privacy responsibilities in their job descriptions.

TOM SCHNEIDER | CISA, CISSP

Is a senior associate of proactive advisory at Cyber Defense Labs, where his current focus includes enterprise risk and cybersecurity assessments. Schneider has extensive experience in IT tech support, cybersecurity and governance.

Addressing Cybersecurity in Job Descriptions

The US National Initiative for Cybersecurity Education (NICE) Working Group has published insightful lists of job responsibilities that include cybersecurity for several different job categories, including leadership, planning, governance, human resources (HR), legal and compliance.[4] In addition, organizations should consider adding cybersecurity responsibilities to position descriptions that are specific to their enterprise.

Examples include:

- **Business managers**—The identification of backup requirements can be listed as a responsibility of business managers, including identifying the servers and databases that need to be backed up (based on the manager's specific department), the number of generations of backups required and their retention periods.
- **IT backup team**—This team should be responsible for initiating contact with business managers to get requirements for the data that business needs to have backed up, configuring the technology to back up the identified infrastructure, and ensuring that the retention and number of generations are consistent with what is requested.
- **Customer service**—Team members should have position descriptions that include compliance with the handling requirements for any personally identifiable information (PII), protected health information (PHI) or other sensitive data that are often processed, such as credit card information.
- **Personnel managers**—Team members should have position descriptions that include ensuring that any

employees who leave the organization are marked as terminated in the HR records system and that any access that they had is revoked no later than the employee's final day at the organization.

As the examples show, for tasks that require more than one team to complete, such as configuring backup tools to be consistent with business requirements, position descriptions can be used to identify which part of the task belongs to which job role.

> "It is not only important to clearly list duties and responsibilities, but it is also necessary to prepare staff to be ready to fulfill these duties through training."

Training Staff on Their Responsibilities

It is not only important to clearly list duties and responsibilities, but it is also necessary to prepare staff to be ready to fulfill these duties through training. Several NIST SP 800-53 controls further identify requirements for role-based training, including AT-3 *Role-Based Training* and its control enhancement, AT-3(5) *Role-Based Training for Processing Personally Identifiable Information*. Role-based training should instruct staff on how to perform tasks that are specific to the roles and responsibilities defined in their job descriptions. Role-based training for processing PII should include training on the types of PII processed and specific handling requirements for it.

In addition to role-based training, other controls in NIST SP 800-53 document the essential security training that should be provided for all staff. Those controls include AT-2 *Literacy Training and Awareness* and its control enhancements: AT-2(2) *Literacy Training and Awareness for Insider Threat* and AT-2(3) *Literacy Training and Awareness for Social Engineering and Mining*. As indicated by the use of the word literacy, the training for control AT-2 is meant to provide the workforce with essential knowledge and competence for security and privacy. Similarly, its control enhancements include identifying indicators of insider threat and recognizing and reporting attempts of social engineering and data mining.

Conclusion

At the most basic level, if management does not make responsibilities clear, then it cannot expect staff to execute those responsibilities. This is true for everyone in an organization, from the most senior levels of management to the most junior staff. The risk of not clearly communicating security and privacy responsibilities is that the tasks to fulfill those responsibilities will not be prioritized and performed. The risk of not training staff for those responsibilities is that then employees will not perform their responsibilities in the way that management requires.

Failing to include security and privacy responsibilities in the organization's position descriptions is essentially confirming staff's belief that, as far as cybersecurity goes, "It is not my job." If management wants to engage its employees in protecting the organization from cyberthreats, this is not the message that it wants to send. Instead, management should use job descriptions to unequivocally communicate responsibilities for cybersecurity and privacy. And management should provide the training needed for staff to effectively fulfill their defined roles in helping to protect the organization from cyberthreats.

Endnotes

[1] National Institute of Standards and Technology (NIST), Special Publication (SP) SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, USA, September 2020, *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

[2] *Ibid.*

[3] National Institute of Standards and Technology, SP 800-53B *Control Baselines for Information Systems and Organizations*, USA, September 2020, *https://csrc.nist.gov/publications/detail/sp/800-53b/final*

[4] National Initiative for Cybersecurity Education Working Group, *Cybersecurity Is Everyone's Job*, USA, October 2018, *https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf*

LOOKING FOR MORE?

- Read *Cybersecurity Fundamentals Study Guide. www.isaca.org/credentialing/itca/cybersecurity-fundamentals-certificate*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*