# Follow a Framework for Enterprise-Wide Cybersecurity

BY STEPHANIE SALAVEJUS, CPP

Over the past two years, cybersecurity crimes against businesses have increased dramatically. Former IRS Commissioner John Koskinen reported that business identity theft cases increased 250% during the first six months of 2017. Several of these data breaches hit close to home for payroll professionals, in part due to business email compromise (BEC) phishing schemes. These attacks were swift and effective because they leveraged the trust and authority of C-level executives within the company. With the objective to be responsive to the request of C-level officers, employees compromised sensitive data with a single click of their mouse, providing a portal for cybercriminals to gain access to employee and sensitive company data.

With today's technology, news media updates are round-the-clock and received almost instantly, but they have little impact on stopping the cybersecurity threats businesses are facing daily. The IRS and the APA alerted payroll professionals in 2016 to be cautious of email phishing schemes that appear

---

*Stephanie Salavejus, CPP, is Chief Operating Officer for PenSoft, an APA Vice President, and the APA's 2017 Payroll Woman of the Year. She is also a member of the APA's National Speakers Bureau, Government Relations Task Force (GRTF), the Board of Contributing Writers for* PAYTECH, *and Co-Chair of the Emerging Technologies Subcommittee of the Strategic Payroll Leadership Task Force (SPLTF).*

to be from within the company, from the CEO, or from a reputable vendor. In 2016, these types of schemes resulted in large-scale theft of personally identifiable information reaching into the tens of thousands. With media coverage of these data breaches, you would think it would be impossible for cybercriminals to launch a successful second attack, but in early 2017, they did just that. The cybercriminals modified their tactics, and the timing of the attacks achieved great success by stealing the information of more than 120,000 employees within the first three months of 2017.

According to a *Forbes.com* article, the Internet of Things (IoT) is the concept of "basically connecting any device with an on and off switch to the internet (and/or to each other)." The IoT has dramatically changed how we do business. The article further states that the analyst firm Gartner says that by 2020 there will be over 26 billion connected devices, with some estimating this number to be more than 100 billion. This in turn requires companies to have solid internal cybersecurity controls and a clear understanding of the security controls and policies of their third-party vendors that manage or act on behalf of the company.

Cybersecurity strategies cannot be the sole responsibility of the information technology or cybersecurity staff. All company stakeholders, including C-level executives, must share the responsibility if there is any hope to mitigate the success of these types of attacks.

## Key Cybersecurity Functions

In light of the most recent breach of 143 million victims, mitigating cybersecurity threats can be overwhelming, but a good first step is incorporating the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF provides straightforward guidelines to help companies identify, implement, and improve their cybersecurity practices.

The NIST CSF consists of the five key functions of cybersecurity, and each of the functions is further broken down for identifying and managing cybersecurity risks:

1. **Identify**—The process of identifying risks throughout all areas of your organization including a risk assessment of data, systems, governance, and access channels to develop a solid strategy for managing and protecting sensitive information. It helps in prioritizing risks and maintaining focus on risk management as it relates to your company's business model. It is impossible to protect what you do not know exists.
2. **Protect**—The development of security controls necessary to safeguard against and deter cybersecurity threats. There is no single solution when it comes to cybersecurity. What works for one organization will not necessarily work for another. Plan to protect your sensitive information similar to the way a tree grows. For each "ring" of protection, you are making it harder for cybercriminals to reach their target—your sensitive information. In the event of unauthorized access, there needs to be a plan in place to contain the threat so that it does not infiltrate the entire network.
3. **Detect**—The implementation of an alarm system to notify you when there is a suspicious activity or breach. The solutions should be proactive, provide real-time notification, and be continually monitored. Employees are a key component in your company's detection system. Educate everyone in the company that if they see something, say something. Also, have a process in place for reporting suspicious activity or behavior and communicate the process to everyone in the company on a regular basis.
4. **Respond**—The development of an effective incident response strategy and team. Your response plan is a dynamic document, unique to your company, that requires updating as your company changes. It should be a detailed roadmap and include identifying key stakeholders' roles in the event of a breach. Key stakeholders may include external parties such as the company attorney, certified public accountant, and media consultants.
5. **Recover**—The development of a recovery plan that identifies what worked and what needs improvement, a communication strategy for both internal and external stakeholders, and process for repairing damage and steps for preventing cybercriminals from unauthorized access to your company's sensitive information.

We all have a responsibility to implement and maintain reasonable data security practices. Conducting routine risk assessments and mitigation exercises will help to ensure your company has strong data security policies. As a payroll professional, you have an important role in reducing cybersecurity threats within your company. The NIST CSF is the starting point for implementing safeguards to ensure that sensitive data does not fall into the hands of sophisticated cybercriminals. ■