BY PETE MILLER

SLOPPY SECURITY COSTS VENDORS

LAX SECURITY PRACTICES CAN KILL A BUSINESS

WANT TO DO BUSINESS WITH Google Inc., Facebook Inc. or Microsoft Corp.? Then it's a must to have strong security and privacy systems. With the advent of the European Union's General Data Protection Regulation (GDPR) — the world's toughest security and privacy standard — and California's sweeping Consumer Privacy Act of 2018, rigorous security protocols are the new normal.

Large tech players won't risk that one of their suppliers or vendors could be hacked, thereby exposing customers' personal information. The potential public relations and legal nightmares could prove catastrophic. In the past, only large vendors and partners had to worry about adhering to such strict privacy and security requirements.

But now, any company that wants to do business with the tech giants must comply. It's especially important for software as a service providers, which large tech firms hire because their service often involves taking private data from customers and storing or processing it using their proprietary tools. Depending on the sensitivity of the data held by the supplier, there are varying levels of security and privacy needed. But as time moves forward, companies should expect to see increased requirements that will build upon past specs.

One common request from large tech companies is to see a vendor's System and Organization Controls 2 (SOC 2) report, a data security and privacy framework established by the American Institute of Certified Public Accountants that focuses on a business' nonfinancial reporting controls related to security, availability, processing integrity, confidentiality and system privacy.

While some businesses already have SOC 2 reports, others do not. If large tech companies do not receive an SOC 2 report from a potential vendor, they may request a laundry list of items they're worried about and ask the company to demonstrate how it will address certain security and privacy risks. In the long run, it's usually easier for a vendor to create a full SOC 2 report, which is then available to include when bidding for work. Vendors also should be able to demonstrate compliance with other globally accepted security standards, such as those outlined by the GDPR, the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST).

Proving adherence to security and privacy standards is more important now than ever. Microsoft during the past 18 months, for example, has really increased its security and privacy requirements for vendors to prove it is GDPR-compliant. It has its own security program required for all suppliers and vendors that handle sensitive information such as personal information, intellectual property and trade secrets. The penalties for not complying are severe, sending fear through the C-suites of many large tech companies. Vendors and suppliers that don't address this now will be left behind while their competitors take over.

How does a vendor or supplier hoping to do business with a big tech firm prepare? First, pick a standard (SOC 2, NIST or ISO) as a framework. Review the list of requirements and map the company's internal controls against that framework. Companies will either have a control that meets that risk perfectly, a control that attempts to meet the risk but isn't necessarily the best practice, or they'll have nothing at all. From there, the company will work to fill in the gaps.

> "THE PENALTIES ARE SEVERE, SENDING FEAR THROUGH THE **C-SUITES OF MANY LARGE TECH COMPANIES.**

Once the controls and policies are in place, and the company believes it is compliant, it will start testing to ensure the security and privacy controls work. The company will work with its CPA firm to identify issues and effective ways to improve.

Once the tests are completed, the CPA firm will write a report that the supplier or vendor could then provide to the large tech firm proving it is compliant. The auditor's report will include a description of the security and privacy requirements within the chosen framework, the internal controls put in place by the company to respond to each requirement, the auditor's test, and the test results. The report also can be an excellent marketing piece for the company, which may use it to generate new business with additional large tech firms.

Companies that become compliant today will face less red tape and hoops to jump through in the future as new rules and regulations are passed. They will be able to respond in a quickly evolving marketplace. SB

PETE MILLER, CPA, CFE, is a shareholder, audit and assurance, with Clark Nuber PS in Bellevue. Reach him at 425-709-6696, or pmiller@clarknuber.com.