How Outsourcing Strengthens Security

It often requires just a series of emails to get senior finance executives to begin looking beyond their own IT departments to safeguard their businesses against cyber-hackers.

No, the messages aren’t from an ultra-persuasive provider of cybersecurity services. In fact, they typically look like they’ve been sent from top management—the CEO or CFO—to a controller containing a request that the recipient wire $25,000 to a certain bank account. As legitimate as the emails appear, they are sent by cyber-criminals on a “phishing” expedition, a scam intended to procure sensitive information (such as credit card numbers and passwords) or money. “In the past two years, our clients have been bombarded by these kinds of malicious attacks, making them more
motivated to take action in the area of security,” says Diego Rosenfeld, Consulting Principal at RSM US. “CFOs and CEOs don’t really have a good understanding of their current security posture—either because they aren’t asking the right questions, or because the IT staff hasn’t put together and articulated a comprehensive security program.”

The more damage their business has suffered, the more urgency company executives will apply to the task of minimizing the company’s vulnerability to cyber-hackers. In any case, they may also feel overwhelmed by the ongoing level of resources required to successfully thwart the fast-moving cyber-criminals. After all, companies face an ever-expanding diversity of malicious viruses—such as ransomware, which infects a system, encrypts specific files, and then demands payment before users can regain access. Executives recalculate the potential consequences of inaction with every high-profile breach (last year’s attack on Equifax exposed more than 140 million consumers) and have likely been urged repeatedly by their lawyers and technology vendors, through webinars and newsletters, to reassess their cybersecurity efforts. “Even at companies where there are folks who have kept up on technology, they may attend a webinar and decide they’d better do something,” says Rosenfeld. “The idea of using managed security services is at the forefront in a lot of conversations we’re having with clients and prospects.”

Experienced executives, many of whom have already contracted out functions like customer support and HR to specialized service partners, naturally gravitate toward exploring their outsourcing options. Given the complexity and ever-evolving nature of the cybersecurity landscape—not to mention the labor shortages throughout the IT function—company executives can quickly appreciate the benefits of having a business partner dedicated to keeping the cyber-criminals out. Some managed services security offerings include video-based security awareness training for end-users, as well as simulated email phishing attacks that measure the training’s effectiveness. (About 90% of all successful data breaches start with spear phishing attacks.) Next-generation managed services providers combine technical safeguards, policies, expertise, operations, and awareness to form a protective shield that would be prohibitively costly for organizations to assemble in-house. In any case, members of the IT function have their hands full managing strategic projects.

Besides, as Rosenfeld points out, among small and midsize businesses it’s common for the IT department to focus on the technical part of cybersecurity—installing firewalls, say—while lacking expertise in the
“There’s a lot of process involved,” says Rosenfeld. “Security is also about how you classify data, the policies and procedures around onboarding and off boarding staff, and how to handle exceptions. There are aspects of cybersecurity that go beyond the technical issues.”

Calculating the payoff on bringing in a provider of cybersecurity services may also go beyond traditional metrics such as return on investment. It’s not feasible, after all, to evaluate the savings that result from a foiled breach. In some cases, it may make sense to analyze the total cost of ownership, comparing using in-house resources to taking on a service provider. “We don’t talk about savings. We’re talking about the fundamentals of IT, the building blocks of having a well-rounded IT department,” says Rosenfeld. “Cybersecurity is now a core function of IT.” For companies that want to pass muster with Fortune-500-caliber customers, it’s also crucial that they have access to the capabilities required to demonstrate adherence to the appropriate compliance frameworks. Such industry-specific standards include: ISO 27001 (information security practices); HIPAA (Health Insurance Portability and Accountability Act); PCI DSS (the Payment Card Industry Data Security Standard, which governs cardholder data); and the recently enacted GDPR (the General Data Protection Regulation rules that protect data-collection for individuals in the European Union).

As advances in such technologies as cloud and mobile continue to reshape their businesses, finance leaders must remain vigilant about identifying and monitoring any new vulnerabilities. As companies grow, they need to ensure that management retains an appropriate level of visibility so that the company can protect itself from cyber-criminals. Each endpoint and entryway must be tightly secured.
At one ambitious non-profit organization, growth started putting a strain on its systems. Non-profits are often required to accept credit cards in multiple ways in order to accommodate different donors or fundraising efforts, thereby creating complex challenges in coordinating vendors and keeping sensitive information secure. “We weren’t capable of keeping up with what we needed to do to best serve the people and communities we were in. We knew we had to get better,” says the CEO of the organization. “It really, frankly, was a safety issue in a lot of ways.”

Having outsourced its cybersecurity to RSM, the business is now “more efficient and safer,” says the CEO. “The result—the bang for the buck—has been more than we could have expected. The technology services they provided truly made us a more effective and efficient organization on every level.”

RSM can ensure that the company’s infrastructure remains sound, and its data secure, as applications evolve and cyber-hackers experiment exhaustively. “We are all drinking from a fire hose as it relates to new security vulnerabilities as well as methodologies and tools,” says Rosenfeld. “The difference is that at RSM, we have people dedicated to research and development. We compile field-based evidence on the efficacy of various tools across a very large and diverse client base.”

Having access to such specialized knowledge may not seem wildly significant to top executives—until they need it. As a non-revenue-generating activity, cybersecurity still ought to be a priority because it can save the business from untold damages in the financial and reputational realm. “If they haven’t been breached before, CEOs and CFOs may not realize how important cybersecurity is,” says Rosenfeld. “They may come to believe that their business is safe. What they have is a false sense of being protected.” Sooner or later, they’ll find that out. But with the outsourcing options they have now, why wait?