ASK THE EXPERT

Cybersecurity: Every business's responsibility

Monumental security breaches at large corporations can dominate the news cycle. But as cybercrime becomes more ubiquitous and criminals become more sophisticated, small companies are increasingly finding themselves targeted. And the fallout can be devastating.

To learn more about the importance of cybersecurity and what small firms can do to protect themselves, Crain's Custom turned to Larry Selnick, director of treasury and payment solutions sales at Webster Bank. A veteran of the banking world, Selnick is well-versed in cyber awareness.

Laurance (Larry) A. Selnick
CTP, SVP, director, treasury & payment solutions sales

Q *Crain's:* Why should businesses focus on cyber issues when they need to run their day-to-day operations?

A *Selnick*: Cybercrime is growing as a real issue for businesses of all sizes and types. Your funds and data can be stolen; your customer relationships and reputation are at risk of being damaged. This is a management issue that needs top-down focus and review.

We provide a Fraud Awareness & Risk Management checklist that goes beyond a top 10 list. It is a tool to assess your internal controls regarding payments, data and key banking best practices. In addition, we provide a Cash Flow Structure chart recommending best practices for your account set-up and internal controls, such as using dual control and system alert notifications. These are all part of an overall education-and-awareness program that highlights why these tools should be used consistently and correctly.

Q *Crain's:* What do business leaders need to focus on first?

A *Selnick*: Education and awareness are key. Employees, key trading partners and service providers need to know cybersecurity is important to help protect your business. Through practice and a process, you will increase awareness and action. This includes what to do, what to look for and how to react if you suspect a cyber issue. Many organizations offer this service, or your leadership team can design your own program.

You need to build a culture of cyber awareness; building a cybersecurity mindset is something you need to incorporate into everything you do, from product design to new-hire orientation. It must be part of the day-to-day process.

Then, focus on what to do if your business is impacted by a cyber event. The simple response is you must have a plan. The size, complexity and scope depend on your business and the impact if you are compromised.

A disaster-recovery plan is all about how to get your operation up and running again, and an incident-response plan deals with any legal ramifications, such as timely reporting to local law enforcement, in a cyber event.

Q *Crain's:* How can I afford to protect my small business?

A *Selnick*: A small business cannot assume that it will go unnoticed. Yes, the news talks about large breaches, but cybercriminals also target smaller business that may not have the IT capacity or leadership focus needed to prepare for and prevent potential cyber risks.

Creating layers of security and seeking specific advice on what those layers might be from your IT, legal, accounting and banking partners is a must! Consider using cyber-liability services that include cyber-response coaches; all will help increase awareness and suggest controls to limit cyber breach impacts. These are all steps you must afford.

An example is using dual control and alert notifications offered in your online banking system—these functions usually come without additional cost and offer increased protection against fraud.

Q *Crain's:* Some small businesses may feel that cyber insurance is expensive and really doesn't cover much. What should they do next?

A *Selnick*: As with any insurance, you are preparing for what might happen. We do not sell insurance, but I have seen clients impacted by hacking, social engineering and other cybercrimes recover with the help of a well thought out cyber-coverage plan.

Do not limit your review to traditional insurance providers. Many providers and systems may offer protection and support for transactions within their system. For example, our merchant services provider offers a security program to ensure your data is safe and Payment Card Industry (PCI) compliant.

Q *Crain's:* We use a lot of new apps on our phones and PCs. We control our lights, track steps for employee health and even use video conferencing on the go. These are not financial or protected data, but should these apps be part of business cybersecurity plans?

A *Selnick*: Without question, you need to engage your IT professionals with a specialty in cyberrisk and controls. The fraudsters may not be trying to steal your money, but they may steal data, such as client credit card info or employees' Social Security numbers and then sell it!

We suggest clients work with their IT teams to build segregated networks to place email, internet and systems holding important information, such as HR data or banking applications, in separate and distinct networks and data files.

Q *Crain's:* What are the risks for companies that don't have an incident-response plan?

A *Selnick*: The requirement of having a cyberbreach plan goes hand in hand with a focused education-and-awareness plan. Your business should already have recovery plans and protections in place that are practiced and reviewed for other potential disasters that could affect your business. What would you do if there was a fire, flood or loss of power? Imagine you can't access your banking systems, or your customer data is "locked" and you cannot access it, or worse, it is ransomed. Planning, communication and practice are just as important for cyberbreach-related incidents.

Start with www.ready.gov/cybersecurity. Your banking, accounting and legal partners probably each have resources you should review. For a copy of our Fraud Awareness & Risk Management checklist, please contact me at lselnick@websterbank.com or (860) 692-1679. ■