The need for vigilance with cybersecurity

The cloud is hanging over us. Five years ago, it might have been sufficient for businesses to manage cybersecurity by banning employee-supplied devices, restricting information systems to “fixed location” devices (like desktops) and encrypting mobile devices that were absolute business needs. These types of aggressive security measures, however, simply aren’t feasible in today’s business environment.

As younger employees raised in the Information Age increasingly overtake the majority of professional positions and social networking replaces the traditional telephone as the primary means of personal communication, employees expect to be able to use modern technologies, like cloud storage, to get work done. Not to mention there is increasing pressure on marketing, communications and sales representatives to utilize social media, and pressure on accounting and finance divisions to provide electronic billing and other e-commerce functions.

Plus there’s pressure on operations professionals to provide informatics on logistics, inventory and other data for predictive purposes. These pressures collectively mount and, as a business leader, you’re eventually forced to embrace technology. What’s the reality? Your business is a part of the world’s network, regardless of whether you would prefer for it to be offline. What businesses often fail to realize is now they’re not just targets, but they’re also tools for attack.

Certainly an HVAC vendor that fixes air conditioning units isn’t at the forefront of the IT industry and isn’t expected to have expertise in cybersecurity. Such vendors don’t have much in the way of sensitive data, and what they do have probably isn’t something organized crime has much interest in. But these vendors are obvious tools for attackers.

In the 2013 Target data breach, the attackers got in via one of Target’s vendors. And this is not the only way a company can become a tool. If you have a network of tens of thousands of devices — and an attacker can penetrate that network and distribute malicious software to those devices — that attacker can use your network to launch an attack. Throughout both my academic career and in the private sector, I have been deeply invested in an ongoing push to secure information systems against such technology-based crimes.

So, how should business leaders respond? They should engage and invest in risk mitigation — informed by the analyses of qualified professionals familiar with the private sector — to determine the proper level of Information Security for their systems. Step one is conducting a risk assessment, and step two is developing a risk mitigation security plan based on that assessment. Instead of focusing on building impenetrable systems like in years past, they should commit to systematically reducing the risks of data insecurity. Security plans should be updated regularly using ongoing risk assessments. Being vigilant will help to chase rainy days away from your company — and your company’s partners, too.