Five Simple Ways to Help Protect Your Business Data as You Would Your Home

BY HIRO IMAMURA, CANON U.S.A.

SAFES, ALARM SYSTEMS, a well-trained pet: these are all things we can use to protect our homes and the valuables inside. Whether a piece of jewelry or an important document, we don't leave our prized possessions lying around in plain sight or behind unlocked doors, as common knowledge tells us that if we do, we're asking for them to be lost or stolen.

Safeguarding the things that matter to you is a fairly straightforward concept — so why is it that many people fail to follow the same security guidelines for their business information as they do for their personal valuables? As new, emerging technologies are implemented almost daily across enterprises, it can leave organizations (and individuals) susceptible to vulnerabilities that could lead to information breaches if the appropriate security frameworks are not in place.

The end of the calendar year is typically among the busiest periods for organizations, which is why October is the perfect time to bring cybersecurity to the forefront of conversations. It also happens to be National Cybersecurity Awareness Month (NCSAM), an annual observance during which public and private sector leaders reinforce the importance of cybersecurity and share insights to help individuals and organizations better understand how they can protect their data.

Many NSCAM tips gear toward consumers and how they can stay safe online — which is great — but businesses should also take this opportunity to revisit their security solutions and protocols to ensure they are adequately prepared. Don't know where to start? Using common safety concepts we use to protect our homes, here are a few simple cybersecurity tips that organizations can put into place to help with these matters in today's workplace.

1. Conduct a safety assessment

When looking to choose a home, it's common practice to research the neighborhood to better understand nearby amenities, resources and of course, safety concerns. You may look into local crime rates and chat with residents to get a sense of the community. When inspecting the home itself, you'll likely make sure windows aren't cracked, doors close safely and securely, and that there is a certain element of privacy. Businesses need to perform this same type of assessment (and do it regularly) to ensure there is security within their digital workplace and identify any critical gaps that need to be filled.

The latest Office of the Future survey seeks to better understand the cybersecurity challenges that partners and customers are facing, and to determine where there is room for improvement. The survey of more than 1,000 U.S. IT professionals reinforced the need for clear cybersecurity protocols that touch every part of the business — from workflow processes to devices and customer interactions. All respondents reported facing a security threat over the past year, with malware and ransomware attacks (57%), compromised devices (49%), web-based vulnerabilities (40%), and social engineering scams (39%) being the most common*. Understanding the top threats is the first step to putting the right guardrails in place to prevent them.

2. Get real-time visibility with an alarm system

With the volume and sophistication of security threats, and the rate at which they are evolving, it's critical for organizations to adopt technologies that create a smarter environment with security features in which employees across all levels can contribute to prevention — no matter how extensive or limited their understanding of the threats and implications. A great move is to invest in hardware and software solutions that have built-in monitoring systems that can alert users to suspicious activity or threats in real-time.

It's critical for organizations to adopt technologies that create a smarter environment with security features in which employees across all levels can **contribute to prevention.**

3. Lock up your valuables

In the case that an alarm system does not stop an individual from entering a home, many homeowners also have a second line of defense in place to attempt to prevent intruders from walking away with their valuables. The simplest examples? A lock or a safe.

Similar to a real padlock, a digital smart lock requires a key or passcode for entry — such as a user authentication system. This is a simple but effective way that organizations can help safeguard information as well as devices such as printers and scanners. Similarly, programs and solutions with data encryption can serve as a digital safe; even if someone gains access to the information itself, they can't necessarily open it.

Given the accelerating pace at which organizations access data, IT leaders must also keep in mind that developing a security framework that safeguards each touchpoint across workflow processes is only the first step. The more data that organizations gather to inform their daily decision making, the more time is required to proactively update and deliver new iterations of these cybersecurity efforts to ensure information does not get into the wrong hands.

No longer need data? Even if data is outdated or not relevant, make sure there are appropriate disposal procedures so they can't be pieced back together later. Similar to a paper shredder you might use in your home, many enterprise devices have security features to delete information — such as an HDD data erase on an MFP that can be set up to erase job data after each task via an overwriting process. These features can provide added protection for employees.

4. Equip yourself, and others

Cameras and safes won't do you any good if you — and those around you — don't understand how to utilize them. This stands true in the workplace as well, as one-third of IT professionals surveyed say technological competence is the top barrier that hinders the adoption of cybersecurity solutions*. While there are solutions with built-in features that allow you to "set it and forget it," security often comes down to the human element. In fact, IT professionals indicated malicious insiders (30%) and human error (25%) as the top security threats*.

According to the Office of the Future survey, employee accountability was reported as one of the major pain points for today's enterprises when addressing cyber threats, with one in four IT leaders indicating that employees have limited or no understanding of threats and prevention. Therefore, it's critical that there is proper, ongoing education so that employees can supplement the security solutions in place by keeping an eye out for things that don't seem right.

5. Invest in your safety now to help limit loss down the road

Nearly nine in 10 IT leaders believe the financial damage from a security breach is either 50% or less of annual revenue*; although ABI Research estimates the number to range between one year and seven years or more of annual revenue depending on the scale of the breach. This is contrasted against the finding that nearly half of survey respondents (46%) reported that their organization's spending on security currently accounts for less than 5% of the company's total IT budget.

This stark underestimation by IT professionals should create a sense of urgency for organizations to take a step back and consider the financial implications of choosing to hold off on investing in adopting and scaling security solutions across the enterprise. We see that these reassessments are happening in the smart home market, which, according to Statista, has seen significant growth in 2019 (18% increase YOY), so why shouldn't we follow suit in the workplace? As consumers invest in the protection of their personal valuables at home, businesses can follow this same approach by equipping the enterprise with the tools necessary to assist with long-term protection of their data and intellectual property.

The intersection of prevention and proactivity

National Cybersecurity Awareness Month is just one month out of the year, but frankly, it's not enough. Given today's complicated security landscape, enterprises cannot afford to wait to evaluate their security efforts, shortcomings and successes once a year; it must be an ongoing and evolving process.

At the end of the day, meeting today's cybersecurity challenges and threats and working to safeguard valuable assets — whether at home or across the enterprise — requires being proactive and taking preventative efforts to stop or help limit a cyber threat or crisis as it arises or before it even happens.

Security is not just an IT issue; just as each individual in a home contributes to the protection of what's inside, each employee in an organization plays an integral role in helping with the protection of the information created and stored there. If each employee understands how to work smarter with the solutions that are available to them and remains accountable, organizations can thrive.

** "Office of the Future" survey, conducted by ABI Research.*

contributor

Hiro Imamura
Canon U.S.A.
usa.canon.com