Small & Midsize Business: SMB Cybersecurity Strategy Depends on Maturity & Resources

Cybersecurity Series

By Mike Caralis, Vice President Business Markets
Verizon Business

What's the difference between small and midsize businesses and large businesses when it comes to cybersecurity risks? Turns out, oftentimes not a lot.

According to the Verizon 2023 Data Breach Investigations Report (DBIR), system intrusion, social engineering (the second largest threat for small and midsize businesses), and basic web application attacks represent the majority of breaches for small businesses (92%) and large businesses (85%) alike. Even how they respond to these attacks has converged over the years, since they increasingly use similar services and infrastructures. Their attack surfaces have more in common than they once did, and as a result their attack profiles can largely overlap. But there is typically one major difference: resources. Resources to pay for recovery from a breach along with resources to proactively protect from an incident. The most scarce resource is the technical expertise in the midmarket space to adequately implement and recover.

Even without the same resources as large businesses, small and midsize businesses should not shy away from embracing technology, but it is essential to acknowledge that while it offers opportunities, it can also come with concerns.

Small and midsize businesses must invest in their people

It's typically harder for small and midsize businesses to recover from breaches. As such, they should do everything in their power to prevent them. One effective way to help accomplish that is by focusing on your people, a critical component of any cybersecurity strategy. According to the 2023 DBIR, the human element factors in the overwhelming majority of incidents and almost three-quarters (74%) of all breaches.

Whether they're guilty of privilege misuse, succumbing to social engineering, or some other human error, employees pose one of the greatest cybersecurity risks. The good news is businesses can do much to help limit that risk.

Small and midsize businesses would do well to establish and maintain a security awareness program to train staff to spot and properly respond to common hacks and other malicious tactics, including phishing, smishing and social engineering. These tactics are generally not sophisticated, but they're effective against careless, unsuspecting or digitally uneducated users. Educated users, however, can identify most of these hacking attempts or at least know what to avoid interacting with, such as unknown users or hyperlinks. Raising the security awareness of one's workforce is especially important if a company employs remote or hybrid workers, who often alternate between personal and professional devices and networks.

Most orgs experience incidents and/or breaches - plan for recovery

While the goal is always to head off threats at the pass, many companies may, at some point, experience a cyber incident. When that occurs, the objective shifts to restoring assets to a pre-incident and trusted state. Establishing and maintaining data recovery practices are essential to help achieve that objective.

An effective data recovery practice depends on a few factors: establishing data priorities and having a realistic assessment of a company's data recovery skills. A startup with very limited resources for implementing security controls may not have dedicated security personnel. Security personnel may double as IT, or the startup may not even have dedicated IT staff. Knowing limitations as an organization is just as important as knowing what the organization is capable of. Making a data recovery attempt with a limited skill set and no plan in place can actually do more harm than good.

Most users shouldn't have access to everything

Managing access credentials and user privileges can go a long way toward limiting the effects of the human factor (in addition to the aforementioned skills training) by compartmentalizing exposure. The importance of access control, using processes and tools to manage access credentials, is underscored by the fact that according to the 2023 DBIR, the most common types of data compromised when small and midsize businesses were breached included credentials (54%) and internal data (37%).

Responding to an active attack

One of the capabilities a more established small and midsize business should first consider incorporating is incident response management, which refers to the policies, plans, procedures, defined roles, training and communications marshaled to prepare, detect and quickly respond to an attack. While the previous strategies focused on prevention or recovery, this approach hones in on responding to an active attack. This is key to help contain social engineering attacks, such as pretexting, which can escalate quickly across a network. Incident response can be effective at preventing lateral compromise, thereby containing a threat that otherwise could have been much more damaging.

Assess your needs and resources, and plan accordingly

The purpose of this article is not to serve as a comprehensive prescription of cyber threat preparedness for small and midsize businesses, but rather to point out that the IT and cybersecurity needs of small and midsize businesses exist on a continuum. Midsize companies may also look into application software security and penetration testing, for example, but it depends on their particular circumstances. It’s up to individual companies to determine their level of cybersecurity maturity and ascertain their hierarchy of Information Technology priorities in order to arrive at a plan that works for them.