citrix

CSO FROM IDG

The SMB Mission: Data Security Without Compromising User Productivity

Experts offer guidance for small and medium-sized businesses on tackling cybersecurity without impacting the user experience.

IDG Communications, Inc. | Sponsored Content

There's little need to belabor the point that the cyberattack landscape has become significantly more dangerous. Yet, for small and medium-sized businesses (SMBs), any security incident can quickly become costly and damaging.

At the same time, it's difficult to limit access to the resources employees need to get work done. Any strain on productivity also affects the bottom line.

So, how do SMB leaders keep data secure without compromising employee user experience and productivity? That's the question we posed to members of the IDG Influencer Network, a community of journalists, industry analysts, and IT professionals who contribute their knowledge and expertise to IDG clients.

"As with many solutions, it is composed of people, process, and technology," says CTO Mike D. Kail (@mdkail).

People Solutions for SMBs

"One of the biggest lessons for SMB leaders is the power of transparency," says Noelle Silver (@NoelleSilver_), Founder of AILI. "User experience is enhanced when the user trusts the 'why' behind technical decisions, especially security. There will always be a trade off when it comes to keeping data secure and keeping users happy, but you can minimize the impact as a leader by being transparent in your decisions and leveraging industry best-known methods."

A common practice is to increase employee awareness about the security basics:

> End-user training comes first. Coaching employees on essential cybersecurity does not cost very much, nor does it absorb a lot of employees' time. Teach what not to click, what to avoid downloading, how to keep data safe, and include password management. — Audrey DeSisto (@AudreyDesisto), CEO, Digital Marketing Stream.
>
> Employees must be trained and reminded to beware of phishing scams and not to overshare personal information on social networks or with any unvetted connections. — Scott N. Schober (@ScottBVS), President/CEO, Berkeley Varitronics Systems.
>
> SMBs can grab low-hanging fruit by educating employees about the basics, like recognizing phishing and social engineering attempts, good password hygiene and governance, and intelligent information security practices. — Gene De Libero (@GeneDeLibero), Chief Strategy Officer, GeekHive

Also, put today's data security into context. "Let them know that just as they can't walk onto a commercial flight anymore, so too can they not indiscriminately use networking resources," says Ben Rothke (@benrothke), Senior Information Security Manager at Tapad.

"In my opinion, the process of keeping data secure is a cultural one, much like the conversion to no-smoking workplaces," says Steven M. Prentice (@StevenPrentice), Technology Integration Specialist.

"Although the no-smoking rule was supported by law, the point is the culture had to be changed to create a new normal," he says. "Cyber-hygiene is not an optional add-on. It must remain a continually reinforced part of a positive work culture, seen not as a compromise but an evolution, and this type of mindset must start at the top."

Process Solutions for SMBs

A solid and regularly updated foundation of user education is underpinned by secure processes. The IDG Influencers suggest that starts with access rights.

"Understanding what level of access employees need to do their jobs and how threat actors exploit user access may help them understand that you are a partner who has their and the business's best interests in mind," says Jason James (@itlinchpin), CIO of Net Health.

Next, apply policies to protect data access.

"SMBs should take a lesson from the failures of much larger organizations and develop, implement, and regularly test a solid but practical cybersecurity policy," says De Libero.

"Cybersecurity doesn't have to be painful or cripple the user experience and productivity," he adds. "For remoter workers, the business can set context-aware access policies that don't add friction to the organization's ways of working."

As you go about setting policies, look at the holistic picture, says Isaac Sacolick (@nyike), President of StarCIO, bestselling author, and digital transformation influencer.

"SMBs need both an outside-in and inside-out view to protecting their data while driving improvements in employee experience and data-driven behaviors," he says. "The outside-in view should concentrate on protecting data from ransomware attacks and other intrusions. The inside-out view requires SMB leaders to implement data governance by identifying data owners, classifying data, determining access privileges, and identifying usage policies."

Technology Solutions for SMBs

The IDG Influencers offered tech guidance — both general and specific — for SMBs to better protect their organizations while not creating too much friction for employees.

Intertwined with the access rights mentioned earlier is identity. "Tying data security to user identities is the easiest, lowest-effort way to modernize security for small to medium businesses," says Kayne McGladry (@kaynemcgladrey), CISO. "Establishing data security based on user identity means that data remains secure regardless of storage location or medium."

DeSisto adds: "Antivirus protection is the starting point to ensure that each of your desktops, laptops, and workstations are equipped with powerful and up-to-date antivirus applications. Secure your system with multifactor authentication (MFA) and guard crucial data, such as your email network and critical CRM infrastructure. Firewalls ought to be in place to monitor internet traffic that flows to and from systems."

Several of the IDG Influencers recommended data encryption:

> Critical data needs to be encrypted, and security protocols need to be continuously updated against continuous threats. Cloud platforms provide much of this protection to a far greater extent than in-house IT teams. However, this does not mean outsourcing security to cloud companies. Data owners ultimately are responsible for the security and viability of their data assets. — Joe McKendrick (@joemckendrick), Analyst and Forbes Contributor.

> Encrypt sensitive data at rest and in transit (for example, BitLocker and TLS). Use platforms that support end-to-end encryption. Ensure that backups are secured with encryption. — Dave Hatter (@DaveHatter), Cybersecurity Consultant.

George Gerchow (@georgegerchow), CSO at Sumo Logic, echoes the need for encryption and says that "collaboration with control" should be the mantra for SMB leaders.

"If you monitor, log and gain visibility into end-user processes it will lead to where and how guardrails are needed," he says. "Single sign-on, MFA, and Quarterly Access Reviews are a great next step. You can then take it deeper with a Zero Trust model that will focus on encryption and data loss prevention."

Bringing it all together

Having overcome the challenges of remote and distributed workforces in 2020, SMB leaders now have an opportunity to bring together people, process, and technology to address data security and the user experience.

"Business leaders need to recognize that technology and security professionals alone cannot provide data security," says McKendrick. "Security is a team effort, and it takes a well-aware and educated workforce to keep security threats at bay."

Visit https://www.citrix.com/fieldwork/ to learn more about SMB solutions from Citrix.

citrix

Citrix Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States