6 Security Controls to Prioritize for SMBs (and One Bonus)

WHITE PAPER

Small and midsize businesses often have enterprise-sized headaches when it comes to cybersecurity, but they typically lack the same resources their larger counterparts have at their disposal to fend off attacks. Here are some tips and hints for SMBs looking to protect their digital assets.

Cybersecurity threats and attacks know no boundaries. They appear in the data center, on the edge of the network, in remote offices and anywhere employees access applications, data or services over the corporate network or the internet. So, organizations without well-staffed security operations centers (SOCs), big Capex budgets or real-time threat intelligence service subscriptions can find themselves behind the eight ball.

For small and midsize businesses (SMBs), the threat vectors are expanding, and the stakes couldn't be higher:

- 58% of malware attack victims are small businesses.[1]
- Cyberattacks cost SMBs an average of more than $2.2 billion in 2017.[2]
- 60% of SMBs say attacks are becoming more severe and more sophisticated.[3]
- 81% of SMBs note that exploits and malware have evaded their antivirus solutions.[4]

1 2018 Data Breach Investigations Report, Verizon, April 2018.
2 2017 State of Cybersecurity in Small & Medium-Sized Businesses, Ponemon Institute, September 2017.
3 Ponemon, Ibid.
4 Ponemon, Ibid.

Devolutions
Devolutions Password Server
TechTarget | Custom Media

One of the best things SMBs can do when it comes to cybersecurity is plan ahead so you can make smart, timely decisions without hiring a boatload of SOC analysts or going to your board of directors to beg for bigger budgets. To help SMBs establish the right security priorities, here's a list of suggestions, along with expert commentary provided by Devolutions' Chief Security Officer:

1. **Secure remote access management.** Your employees are increasingly working from locations outside the traditional headquarters, from their home offices to clients' facilities and public Wi-Fi spaces. Be sure you can manage your employees' access securely, regardless of their location.

   CSO Pro Tip: *Usage of IPSEC and SSL VPNs are highly recommended when it comes to secure remote access. They are easy to deploy and affordable. Cloud services are great for mobility and availability, too, but make sure you understand your risk model and the limits of responsibilities your service provider can provide. Communication links must use strong encryption and authentication.*

2. **Secure digital vault.** As more and more business functions are conducted online, organizations must accommodate and secure everything from employees' passwords to their most vital intellectual property and private records. This is particularly challenging for SMBs, since most have little to no visibility of their employees' password management practices. A secure digital vault can help by allowing employees to securely store passwords and digital credentials, while giving organizations the ability to spot potential problems in how their employees use passwords.

   CSO Pro Tip: *Many successful breaches from the Internet result in instant data loss because confidential and private information was not secured properly. Most SMBs tend to focus on the perimeter only, rather than assuming breach. Protect your information carefully, in-house and in the cloud, with a secure digital vault that uses strong encryption and authentication.*

3. **Secure password management.** In today's business climate, organizations are going digital on access to all kinds of resources, from software applications to building entrances. Many of those resources lack traditional cybersecurity defense frameworks, and you need an approach that lets the good guys in but keeps the bad guys out. We've mentioned password management earlier in this paper, and password security also goes hand in hand with access management. This covers a wide range of applications and use cases, such as ensuring that proper credentials and privileges are being applied; that flexible, automated policy management is in place as employees change roles; and that identities are verified when employees log into applications, databases and cloud services—or even try to enter the building during off hours.

   CSO Pro Tip: *Password-protected spreadsheets and other single-user-oriented password management solutions have proven inefficient for organizations. These solutions are hard to manage and are limited in security features. A centralized, secure and flexible solution will prevent, or at least limit, the impacts of potential breach, or attack from a disgruntled employee.*

4. **Multifactor authentication.** Passwords aren't dead, but they're not the only step you need to take to enable security. SMBs need to come up to speed on digital keys, biometrics and other complements to traditional passwords. If you're only relying on passwords, you're significantly at risk. (And don't think your employees are fooling anyone by using "password" as their password, or placing the ubiquitous Post-It note with their password in plain sight on their desk. Multifactor authentication is the way all SMBs must go.)

   CSO Pro Tip: *Multifactor authentication on the perimeter is not even an option nowadays. Online password brute-forcing and password spraying techniques are widely used by attackers in attempts to guess user credentials. These attacks are common and happen daily—even on Outlook 365. They know your corporate e-mail addresses; they are not hard to find or guess. Internal vital services are also overlooked when it comes to strong authentication. Protect your vital assets with a true second factor, combining something you know with something you have or something you are.*

5. **Automate, automate, automate.** There is a massive and growing chasm between the number of cybersecurity job openings and the amount of qualified individuals to fill those slots. Of course, you should make hiring top-notch cybersecurity talent a priority (either for internal staff or through outside experts), but you

will not solve this problem simply by ramping up college recruiting or poaching your competitors' cyber-talent. New tools are making it easier for smaller organizations to handle big-company security problems without having to hire an army of security engineers or staff a massive SOC. It also mitigates security issues involving human error.

CSO Pro Tip: *Automation is a powerful ally for enforcing end-to-end security while preventing potential human error. It can also speed up incident responses and overall security operation performance. This value is added not only to security functions, but also to operation functions. While automation offers a direct return on investment, putting it in place requires skillful professionals (DevOps/DevSecOps) and the right tools. We recommend hiring an automation expert for both optimizing normal operations and security controls to optimize value of automation.*

6. **Educate your end users.** Security best practices—in general, for all types of SMBs, and specifically for the unique circumstances of your organization—need to be clearly and consistently communicated. That communication may often come from your CISO or your sysadmins, but it must also be supported in a compelling and visible way from your business leadership. Your corner-office executives, including your CEO and even your board of directors, have to make it very clear that cybercrime is a major threat to the organization's well-being, and that taking the right steps to ensure cybersecurity is everyone's responsibility, not just the SecOps team.

CSO Pro Tip: *Security is everyone's business, and end users have a key role in securing an organization. Your end users are common targets and participate in overall detection, prevention and impact mitigation of security incidents. However, for them to fulfill their role, they need to adopt the management's commitment on security and be trained properly. A well-executed end-user security awareness plan will entice your audience to follow corporate procedures, report anomalies without fearing sanctions and actually help your technical team to resolve issues.*

BONUS TIP FROM THE CSO

Understanding and measuring risk. All these previous controls will help your organization to mitigate cybersecurity risks from outsider and insider threats. However, the same questions will come back again in every meeting within senior management and board of director circles: "Where is our return on investment? Are we gambling with money that could be more useful elsewhere? Will it slow down operations?" If your cybersecurity program is not well understood and adopted by the board of directors and other members of the senior management, it will fail to have enough budget and support.

To get support and budget, enterprise risk appetite (the will to take risks) and risk tolerance (maximum permitted risk) must be clearly defined by business owners, boards of directors and senior management. Then, organizations' threats must be evaluated according to those limits to determine what are unacceptable risks, and prioritize their treatment. For businesses not familiar with that practice, it has been proven to be quite effective when performed with experienced partners specialized in risk assessments. That way your upper management will better understand security risk and, therefore, your budget requests. Risks are generally expressed qualitatively as high, medium or low. But, you must insist on quantitative measurements to define your risk. For example, a high risk might be a loss over $1 million or negative global media exposure. This is particularly helpful for decision makers to understand monetary and reputation impacts rather than: "Your e-mail account will be hacked."

ACTIONABLE ADVICE AND QUALITY TOOLS FROM A TRUSTED ADVISOR: DEVOLUTIONS

No SMB can go it alone when it comes to cybersecurity—nor should it. That's why working with a trusted third party that is both technically adept at cybersecurity and understands how to implement and manage cybertechnology tools and services in a real-world business context is essential.

Devolutions offers SMBs a wide range of technology solutions to ensure data, applications and services are secure and available even in the face of increased number, diversity and sophistication of cyber threats. For nearly a decade, Devolutions has helped countless smaller organizations become more efficient through innovative management tools that allow their employees to work flexibly, yet securely—from the data center in a headquarters facility to a Wi-Fi-enabled coffee shop connection to the cloud.

Among Devolutions' relevant offerings are:

- **Devolutions Password Server,** a password management system for both privileged and business users that helps reduce unauthorized access to critical assets and prevent insider attacks
- **Remote Desktop Manager,** a privileged access management tool that tamps down on risks associated with insider threats and data breaches, while helping to ensure governance, audit and compliance requirements.
- **Devolutions Cloud,** a highly secure portal to a wide range of cloud services, including user databases, online backup and more.
- **Wayk Now,** a remote access management platform that facilitates remote support of user problems and ensures secure connectivity using strong TLS 1.2 with user validation.

For more information on how Devolutions can help SMBs like yours protect against the mounting cybersecurity threat vectors, please visit https://devolutions.net.