



Small- and Mid-Sized Businesses Are Under Cyber Attack





Contents

Intro	3
SMBs Are Attractive Targets.....	3
Most Common Attacks on SMBs	4
Results of an Attack Can Be Devastating.....	4
The Best Defense is a Good Offense	5
The Convenience of Single Sign-On	5
The Power of Multifactor Authentication	5
Five Additional Best Practices to Enhance Security	6
1. Conduct an Online Security Risk Assessment	6
2. Discuss Devices and Re-Evaluate Permissions	6
3. Identify Accessible Information	6
4. Establish a Back-Up and Recovery Data Plan	6
5. Train and Educate Employees	6
The New Normal for Today's SMBs	7
About Digital Resolve.....	7





How Multifactor Authentication and Single Sign-On Technologies Work Together To Protect Your Organization



43%
of SMBs are
the target of all
cyberattacks



Only 28%
of SMBs say
they are “very
concerned” about
these threats.

As cyberattacks become more prevalent, it is very apparent that small- and mid-sized businesses (SMBs) are becoming a more appealing target than ever before. While SMB cyberattack stories don't seem to be making the top headlines, a disturbing trend is escalating in the background.

Before the coronavirus pandemic, the U.S. Small Business Administration, reports **there were 30.2 million SMBs in the United States, employing almost half (47.5 percent) of the nation's workforce.** This same group is **the target of nearly half (43 percent) of all cyberattacks,** according to the Verizon 2019 Data Breach Investigations Report, and represents the largest share of the total number of attacks in the report. Equally disturbing is the fact that 56 percent of these breaches take months or longer to discover.

In another study, a staggering **85 percent of managed service providers (MSPs) reported attacks against SMBs over the last two years, compared to 79 percent in 2018.** However, the disconnect comes in the fact that only 28 percent of SMBs say they are “very concerned” about these threats. The reality is that they should be.

SMBs Are Attractive Targets

SMBs tend to be easy targets as they do not have the resources and infrastructure in place that larger enterprises have to identify attacks, alert and/or block an attack using pre-set security protocols and multiple technologies. Limited IT staff, little focus on cyber security, insufficient proactive planning, and lack of adequate staff training to mitigate human errors are also key factors. In defense of SMBs, many operate on much smaller budgets and do not have the resources necessary to not only develop the proper infrastructure, but also to swiftly react once an attack has occurred.

While any industry can easily be a target, SMBs that work within the public, healthcare and financial services sectors present the greatest opportunities for cyber criminals. All of these industries deal with a significant amount of sensitive data and information that could prove valuable to a potential cybercriminal. But, remember, cyber criminals are creatures of opportunity so they are constantly looking for “low-hanging fruit” which means any SMB providing online access to employees, partners, vendors, customers, etc. is at risk.

Most Common Attacks on SMBs

Not only are the attacks on SMBs increasing in frequency, they are improving in quality. The attacks logged in the Poneman 2019 State of Cybersecurity for SMBs Report notes that attacks are sophisticated and involve actions such as targeted phishing emails aimed at employees or a single focus on hacking to obtain specific company data.

The most common type of global cyberattack is phishing something that 57 percent of SMBs worldwide fell victim to this past year. Stolen and compromised devices came in at 33 percent and credential theft was also a common avenue of attack. As an example, for a phishing attempt to be successful, an email must pass through software filters and then be acted upon by the recipient, then exposing sensitive information such as passwords to provide access. While that may sound difficult, the Valimail Spring 2019 Email Fraud Landscape report indicates at least 3.4 billion fake emails are sent each day. For this reason, companies need the ability to quickly investigate any and all security and compromised data incidents.

Another type of increasingly concerning threat is the ransomware attack. Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Cybersecurity Ventures expects that a business will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019. This makes ransomware the fastest growing type of cybercrime.

Internal threats should also not be dismissed. While the obvious concern is to look outside an organization, an employee could lash out in anger and delete critical files or act more maliciously to harm the company by infecting its systems with a virus. Additionally, recent developments such as the Bring Your Own Device (BYOD) to work and the proliferation of Internet of Things (IoT) devices within the corporate environment could unintentionally expose a company to additional risk.

A solid security plan should cover both potential internal and external threats.

Results of an Attack Can Be Devastating

According to the Poneman report referenced earlier, the most common result of cyberattacks is data loss, with 69 percent of the companies in the United States reporting they lost some sort of sensitive personal information belonging to employees or customers. This is a 50-percent increase since 2016.

While some SMBs may try to fly under the radar, the stakes are very high, and the results can be costly. According to Cisco, the average cost for SMBs recovering from cyber breaches is \$500,000, with some SMBs reporting they incurred costs as high as \$1 million to \$2.5 million following a cyber incident. And, many do not ever recover. According to the U.S. National Cyber Security Alliance, 60 percent of small companies are unable to sustain their business more than six months following a cyberattack.



**Business will
fall victim to
a ransomware
attack every
11 Seconds
by 2021**



**The average
cost for SMBs to
recover from cyber
breaches is
\$500k**

The Best Defense is a Good Offense

The best security strategy when dealing with cybercriminals is to be proactive. The good news is that there are enterprise-level cybersecurity solutions that are now within reach for SMBs from both a cost, implementation and convenience perspective.

Confirming someone's identity has become a necessity for SMBs around the world as they take more of their business activities online. The majority of IT professionals would be the first to tell you that controlling access and verifying user identities are two things that keep them up at night.


More and more companies have thankfully turned to multifactor authentication (MFA) to provide a necessary level of secure corporate access based on multiple data parameters and other factors derived from end users' login attempts. However, less technically advanced versions of MFA often disrupt the end-user experience and, used as a standalone, have not proven to be enough to identify and stop today's chameleon-like fraudsters from unauthorized access to sensitive data and personal information. Until recently, it's been a struggle to find a convenient AND secure solution to thwart these cyber criminals. However, Digital Resolve offers a proven, cost-effective Single Sign-On (SSO) solution with its own proprietary MFA technology built in.

The Convenience of Single Sign-On

SSO technology has emerged recently that allows SMBs to more easily manage access to sensitive data while giving users a simplified way to manage logins with one click, and only one set of credentials. SMBs are constantly challenged with ensuring 24/7, secure access to information across a multitude of disparate technology platforms, systems, applications and devices. On average, business employees manage nearly 200 individual passwords. SSO provides a much-needed balance of benefits not only for the business itself, but also for end users requiring corporate access, whether they are employees, clients or partners.

The Power of Multifactor Authentication

Now more than ever SMBs are under immense pressure to prevent unauthorized access to sensitive data and personal information. Multifactor authentication is one of the most effective ways to securely manage that access. While the basic concept is simple, the benefits are great. With multiple layers of authentication in place, hackers can be proactively prevented from accessing company accounts, data, networks and systems even if they have somehow obtained a single password. Digital Resolve's offering also combines behavioral profiling, device identification and calculated risk factors to automate the authentication process with transparent yet powerful protection that's hard to bypass—no matter how seasoned the criminal. Should a login attempt be deemed suspect, adaptive authentication options spring into play to provide robust protection that's hard to bypass—no matter how seasoned the criminal.

A woman with brown hair tied back, wearing a blue denim shirt and a dark leather apron, is smiling at the camera. She is standing in what appears to be a workshop or garage, with various tools and equipment visible in the background.

Now more than ever SMBs are under immense pressure to prevent unauthorized access to sensitive data and personal information.

Five Additional Best Practices to Enhance Security

Building and maintaining a security plan against cyberattacks should be at the top of the priority list for any SMB, especially if they expect to survive in today's digital marketplace. Outside of deploying proven, cost-effective technology solutions, there are some additional best practices that SMBs should put in place to further strengthen their security posture against cyber criminals.



1. Conduct an Online Security Risk Assessment

Determine what or who could threaten your network and assets (i.e. cyber criminals, disgruntled employees, malware, etc.) as well as the likelihood of it occurring. Estimate potential damages in each case. Rank which threats are the most important to protect against. Based on the identified security risks, evaluate the current solutions in place to provide protection against these threats. Identify any gaps in protection.



2. Discuss Devices and Re-Evaluate Permissions

Mobile devices, such as smartphones and tablets, and the IoT continue to help drive business. Plan for how and when different devices will connect to your online network beyond the desktop. Assess current and potential online users to determine who has permission to access different types of data and information. Re-evaluate who should have that access as well as the type of access (i.e. read only, administration, etc.) they should have.



3. Identify Accessible Information

This includes not only corporate data and other information but also employee, customer, partner, vendor and bank accounts. Determine which contain private or sensitive information. Conduct a thorough audit of all the transactions conducted online through your network, including those involving benefits, downloads, ecommerce, payments, banking, scheduling, etc.



4. Establish a Back-Up and Recovery Data Plan

While it may seem obvious, this is a proactive stance that many a SMB overlooks. You should have a set system that automatically backs up data on a regular basis. Similarly, you should make sure your network is set to automatically check for the latest updates to make sure your company is always protected. This includes programs as well as antivirus programs that can identify and block ransomware and provide real-time protection against software threats like viruses, malware and spyware across email, apps, the cloud and the web.



5. Train and Educate Employees

Human error will continue to drive data breaches so make sure both you and your company employees stay up to date on the latest security threats. Take actions to educate your staff about how to handle suspicious emails and critical company data.

Additionally, as cyber liability becomes a reality for SMBs, you may want to consider cyber insurance for additional protection given that many SMBs simply do not recover financially from a single cyberattack. Prior to researching the options, review your business insurance coverage first. If your organization has standard business insurance coverages such as General Liability, Professional Liability, or Errors and Omissions, then find out whether you are covered for losses related to data breaches or cyberattacks.



The New Normal for Today's SMBs

The current statistics show the odds are quickly stacking against SMBs as they are considered one of the most vulnerable targets out there for cybercriminals. However, with proactive planning and protection, SMBs can make certain their team is educated and armed with the right technology and tools to protect their company and data from the cyber crook looking for his or her next victim.

Employing strong, reliable and frictionless security now represents the new normal for today's SMBs.

About Digital Resolve

Since 2004, Digital Resolve has delivered solutions that help companies maintain trust and confidence among their audiences through proven and cost-effective fraud-protection and identity intelligence technology. The Digital Resolve platform provides the industry's only solution that couples its proprietary and substantiated multifactor authentication (MFA) and behavioral monitoring technology with its own single sign-on (SSO) capabilities to deliver proactive protection that secures online accounts, information and transactions from login to logout. For nearly 15 years, enterprises across a number of industries, from financial services to fast-growth technology to small- and medium-sized businesses to healthcare, have benefitted from having a single, easy-to-deploy solution that provides comprehensive security for online users.

Visit digitalresolve.com for more information on the Digital Resolve platform of solutions. Follow us on LinkedIn and Twitter. Headquartered in Atlanta, Digital Resolve is a division of Digital Envoy Inc.

Contact Digital Resolve

Contact us to learn how the Digital Resolve platform can provide real-time protection against potential risks for your business.

6525 The Corners Parkway NW
Suite 400
Peachtree Corners, GA 30092

(+1)678.258.6300 www.digitalresolve.com

