

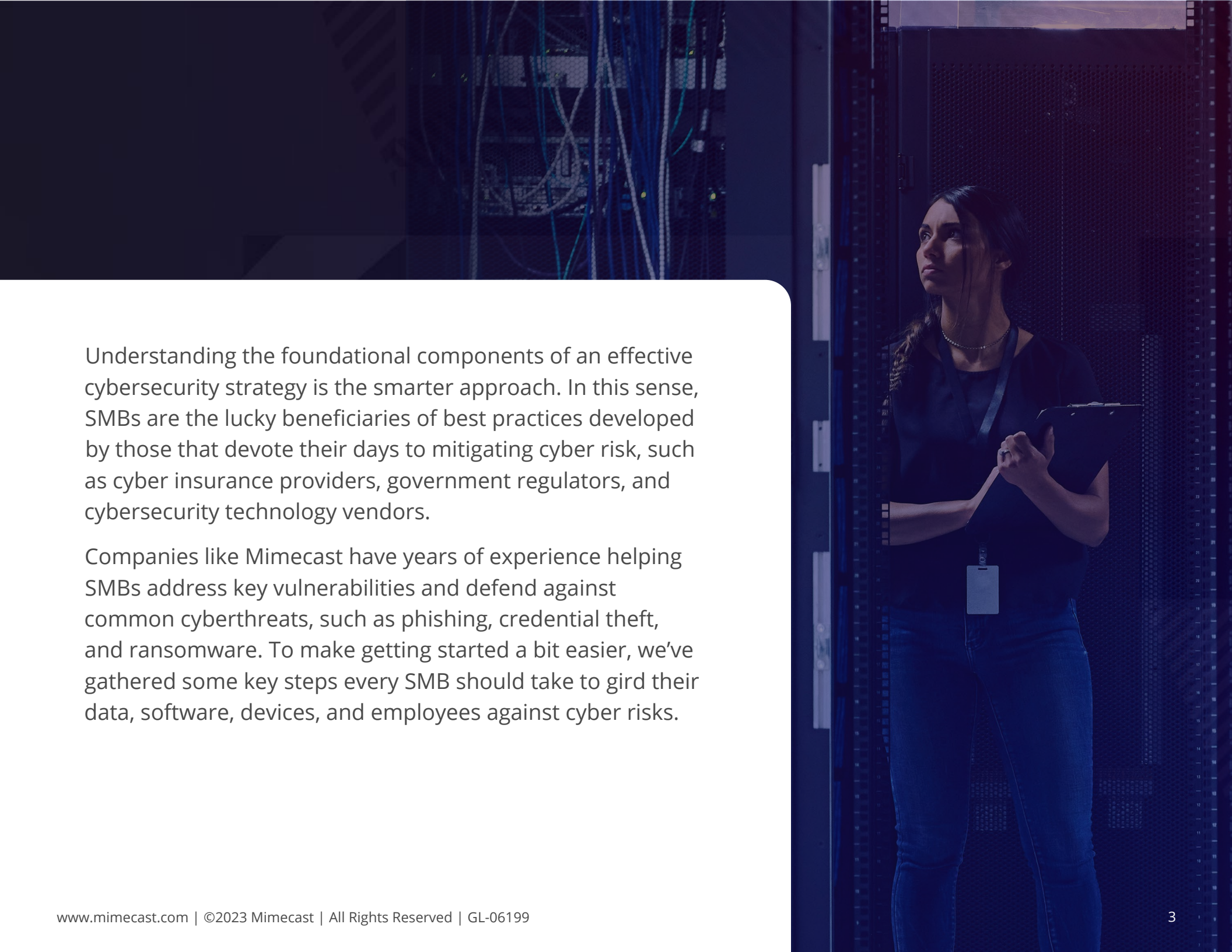
# 7 Cybersecurity Steps Every SMB Should Take

*Small to midsize businesses (SMBs) can be overwhelmed in the face of increasing cyber risk. These seven steps can help them bolster their defenses.*

**There's no doubt that small to midsize businesses (SMBs) are at increased cyber risk. What's less clear for many SMB leaders is where to begin in building up their cyber defenses.**

With limited budgets and often minimal cybersecurity expertise, smaller organizations can be challenged with putting in place the necessary controls.

And in today's uncertain economy, SMB leaders may be tempted to put off cybersecurity planning and investments. But tough times are, in fact, some of the highest risk periods when it comes to cybercrime, so kicking the can down the road would be ill-advised.

A woman with long dark hair, wearing a dark blue top and jeans, stands in a server room. She is holding a clipboard and looking upwards and to the right. The room is dimly lit with blue light, and server racks are visible in the background.

Understanding the foundational components of an effective cybersecurity strategy is the smarter approach. In this sense, SMBs are the lucky beneficiaries of best practices developed by those that devote their days to mitigating cyber risk, such as cyber insurance providers, government regulators, and cybersecurity technology vendors.

Companies like Mimecast have years of experience helping SMBs address key vulnerabilities and defend against common cyberthreats, such as phishing, credential theft, and ransomware. To make getting started a bit easier, we've gathered some key steps every SMB should take to gird their data, software, devices, and employees against cyber risks.

## Where to Begin: 7 Essential Steps

Large enterprises often have entire departments dedicated to cyber protection and risk management, led by seasoned CISOs with years of experience in the field. This is not the case for **SMBs, which are limited in their resources**. Yet companies of all sizes have some common areas of focus when it comes to creating an effectual cybersecurity strategy. And SMBs don't necessarily need a million-dollar budget to address their biggest vulnerabilities and threats. In fact, SMB leaders can take a few relatively straightforward actions that can prove very powerful in mitigating their organizations' cyber risk.

On the following pages, we outline seven essential steps SMBs can take to bolster their defenses.



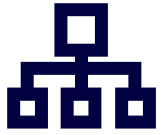


## 1. Designate a cybersecurity point person.

**Giving one individual primary responsibility for implementing cybersecurity best practices is one of the most important actions a business leader can take.**

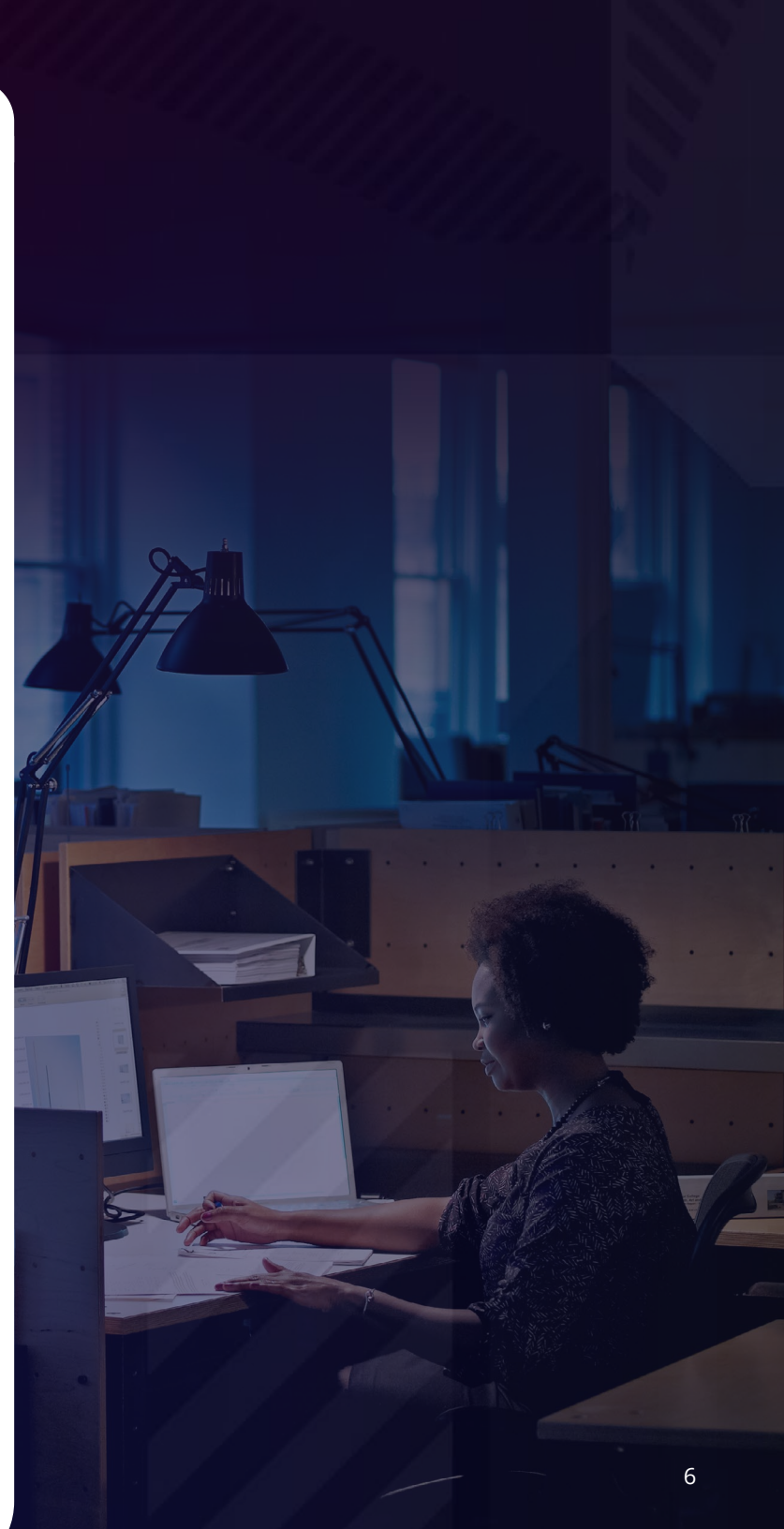
Cybersecurity expertise does not have to be a prerequisite, but an appreciation for the importance of cyber protections and an intellectual curiosity about the subject matter is. Those with an affinity for technology, risk mitigation, or program management can be ideally suited for such a role, overseeing the creation of a well-rounded cybersecurity plan, and reporting on progress and results on a regular basis.





## 2. Develop and practice an incident response plan.

Creating a formal, written incident response plan that specifically lays out what the organization will do to respond and recover from a cyberattack is not only a good idea, it's a prerequisite for most cyber insurance policies. Taking the time to develop this plan, with input from relevant stakeholders throughout the organization before something happens is key. The plan should cover how the organization will contain or eliminate identified threats, as well as what steps it will take to maintain operations during and after an incident. Conducting tabletop exercises to practice organizational responses to simulated attacks will help everyone become more comfortable with the response plan and their roles in it.





### **3. Conduct regular, timely training for all employees.**

It's critical that SMBs enlist their workforce as a primary line of cyber defense. Human error remains the biggest factor in a successful cyberattack.

**The only true antidote to risky behavior and poor cyber hygiene is regular security awareness training and human risk assessment.**

Email and collaboration tools have become an easy way into a company's networks, and cybercriminals are all too eager to exploit them. Educating employees about the latest social engineering and phishing techniques being deployed against organizations empowers them to identify common email red flags, for example. They also will know what to do when they encounter something suspicious. Remember: Everyone should participate — even and especially the CEO.



## 4. Invest in identity management.

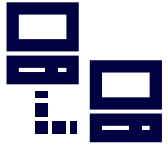
As one CISO recently told us, “Identity is the new firewall.” Companies of all sizes have embraced hybrid and remote working and the cloud-based systems that make productivity software (such as email and collaboration tools) available anywhere. This focus has rendered perimeter-based protections – focused solely on detecting network intrusion – inadequate for a strong cyber defense. It’s still critical to safeguard networks, of course: More than eight out of 10 cybersecurity attacks are now enabled by stolen or compromised credentials, according to a recent report by Mimecast partner CrowdStrike.<sup>1</sup>

Armed with these usernames and passwords acquired via credential harvesting, phishing, or social engineering, bad actors can enter a network through the front door, reset an individual’s user profile to add more access privileges, move around the network, and do all kinds of damage. Some proven best practices to mitigate this risk include requiring good password hygiene, implementing multifactor authentication, and implementing an identity access management (IAM) system, which, in conjunction with a secure email gateway, can block the exploits cybercriminals use to steal credentials.

---

<sup>1</sup>“CrowdStrike 2023 Global Threat Report,” CrowdStrike





## 5. Back it up.

The threat of ransomware persists and continues to evolve as cybercriminals adapt to overcome companies' bolstered protections. Having a playbook that can be put in action the moment a ransomware attempt is detected is crucial to minimizing impact, as is cybersecurity awareness training. Just as important is data backup and disaster recovery, particularly as ransomware gangs have expanded their focus on data stored in the cloud.

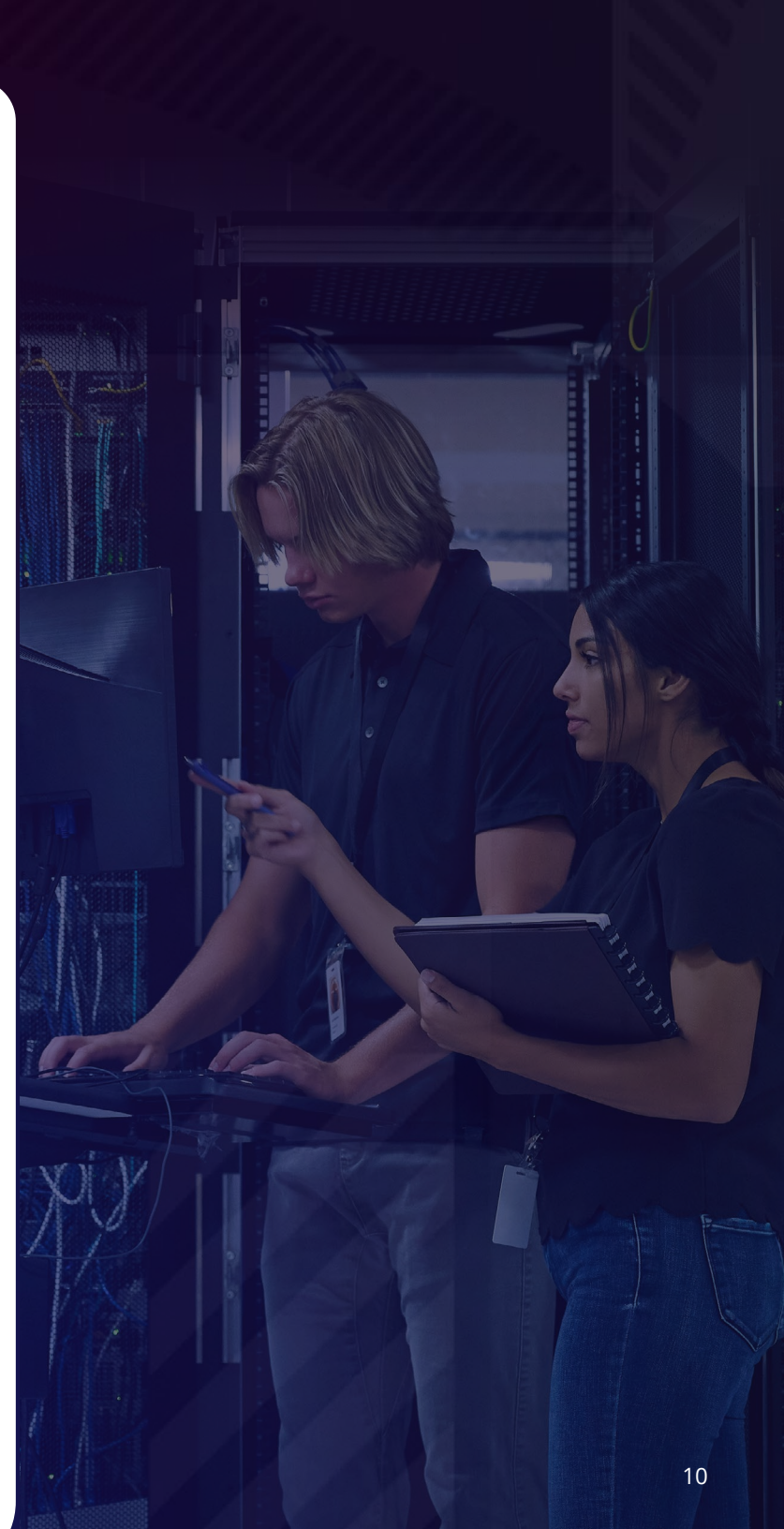
The ability to restore data in a timely fashion is the key to minimizing the impact of ransomware and other types of cyberattacks. **SMBs should invest in regular data backup and archiving** for all of their important systems that not only deliver the required level of business continuity in the event of a cyberattack – but – because cybercriminals may specifically target backup data to prevent recovery, are themselves protected against an attack or other outage. SMBs should also review and test these backups on a regular basis. Commercial backup solutions and services can help SMBs protect their data crown jewels.



## 6. Perform regular patch management.

Cybercriminals track and take advantage of known vulnerabilities in business software, using this weakness to access a corporate network. A patch is a software update that remediates vulnerabilities that have been discovered. A consistent approach to patching software and operating systems is an important aspect of multilayered protection against ransomware and other exploits, yet all too often, companies fall behind on patch management, particularly if they rely on onerous, manual processes to do so. Patch management tools can prioritize vulnerabilities and automate the assignment of patch management tasks, increasing the likelihood that an SMB keeps its software as updated and secure as possible.

*Note: If your software vendor is no longer offering patches and updates for its product, it's time to find a replacement. End-of-life software poses serious cybersecurity risk.*





## 7. Secure email and other communication channels.

Email and collaboration software are essential to the operations of any modern business, and SMBs are no different. But they also offer the easiest entry point for cybercriminals.

**More than 90% of cyberattacks – think: phishing, credential theft, ransomware, and zero-day attacks – start with email.**

Most SMBs rely on popular business platforms, such as Microsoft 365 and Google Workspace, for email and collaboration. But with their massive customer bases, these solutions have become primary targets for bad actors who can increase their return on attacks exponentially by focusing on vulnerabilities in these broadly adopted tools.

While a small business owner might assume that cloud systems from major technology vendors provide adequate cybersecurity out of the box, a stream of recent news stories about successful cyberattacks originating via these email and collaboration systems indicates otherwise. SMBs should earmark budget to invest in secure email and collaboration solutions designed to identify and neutralize common threats.

## In Conclusion

By taking the actions laid out in these important seven steps, SMB leaders can create a solid foundation upon which they continue to develop a robust, multilayered cybersecurity defense. For companies that have already implemented some of these steps, reviewing and revising them at a regular cadence can help them keep pace in an ever-evolving cyberthreat landscape.

For even more information, [read how](#) Mimecast's Cloud Integrated product can help SMBs protect one of the biggest vulnerabilities: their email systems.