Acronis

Cyber resilience: uncovering strategies and technologies

Anticipate, withstand, and recover from modern cyberattacks – no matter what

If you're like most SMBs today, your company's data is your biggest asset.

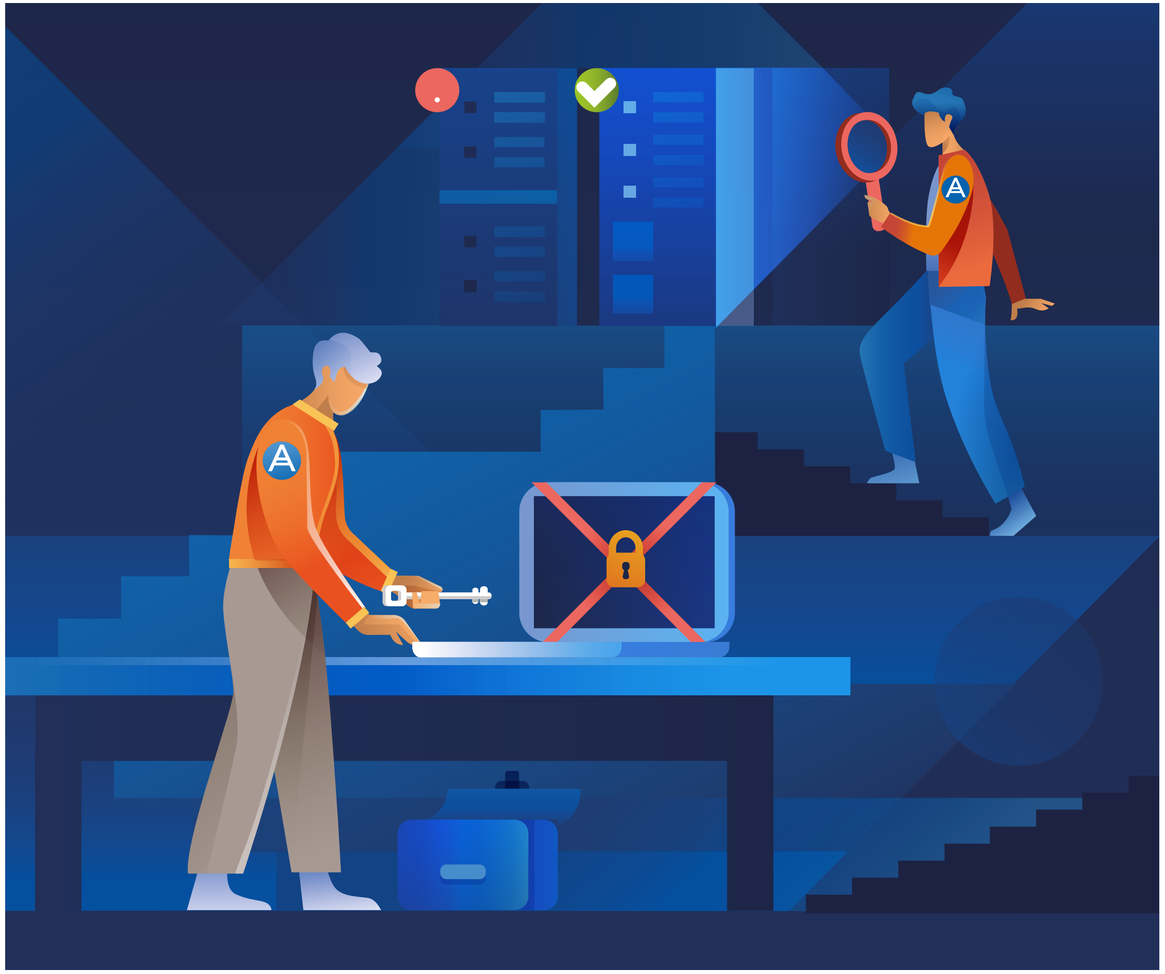
Today's businesses would be unable to keep going and maintain a competitive edge without embracing open standards and fast communication. These have been especially useful to small and medium-sized businesses (SMBs), allowing even the smallest companies to compete with much larger players and scale to meet global demand. Yet these same technologies have also created more vulnerabilities than ever before.

For many businesses, downtime is simply not an option—but just saying so won't make this a reality. The old adage that "failing to plan is planning to fail" is even more true when it comes to security. Without strategies and technologies already in place before disaster strikes, the possibility of graceful recovery and restoration of operations is just a distant dream.

Unfortunately, the ever-evolving nature of today's threat landscape presents a greater challenge to today's organizations that rely on data. Today's SMBs need concrete resilience strategies to help them avoid growing pains and reduce their vulnerability to threats.

In this ebook, we'll explore the threat landscape, including recent changes to the field of cybersecurity; we'll then examine the definition of cyber resilience and look at five core strategies to help businesses build and enhance their resilience in the face of today's threats.

Threat Landscape Overview



Despite the troubling headlines, few people who aren't directly involved in security are aware that over the last few years, cyberattacks have become big business. Estimates indicate that we're already paying about $20B a year in ransomware payments worldwide, a number expected to rise to around $265B within a decade.

Average payouts have also gone up by over 171% in the last two years, to over $300,000. Yet ransomware, while increasingly common, isn't the only type of attack out there. Malware, which can shut down operations or cause dangerous critical failures; denial of service, which can render products and services completely nonfunctional or inaccessible; and data breaches, which can steal confidential data worth far more than a ransom payout, are just three more major types of threats that are becoming increasingly commonplace.

The FBI's Internet Crime Complaint Center (IC3) reports that there were 791,790 complaints of cyberattacks in 2020, leading to $13.3B in losses in the U.S. alone. Attacks reported include phishing, extortion, data breaches, and identity theft. There has also been a rise in the use of automation to create more powerful and sophisticated attacks, including credential stuffing, denial of service, and exploit kits, which allow anyone to establish their own cybercrime business.

Smaller businesses are at particular risk. According to the U.S. Small Business Administration, "88% of small business owners felt their business was vulnerable to a cyberattack," yet these are the very companies that usually lack a comprehensive cybersecurity team or even the knowledge of where to begin mitigating the threat.

Security has become an even bigger concern over the last few years due to a few additional factors:

Today's hackers are no longer the iconic "guy in a black hoodie." They are sophisticated, well-funded, and well-equipped—and they're going after your data.

COVID "Cyber pandemic"—chaos, confusion, weakened infrastructure and management chain (and also turning medical and pharma companies into major targets)

Price decreases for AI and bot tools, making these available to hackers

The rise of nation-state actors, particularly the "big four": China, Russia, North Korea, and Iran

Think you're too small as an SMB to attract hackers' attention? What's become clear from headline after headline is that no organization is immune. From small businesses having their hard drives wiped and their data held for ransom to major industrial operations having their production lines hijacked, surviving in this threat environment means being able to predict, withstand, and adapt to challenges.

Measures of Cyber Resilience

For many—if not most—SMBs, data is the beating heart of their business. And protecting that data is the key activity of cybersecurity. In IT terms, there are five factors that you need to take into consideration to create a truly comprehensive security posture: Prevention, Detection, Response, Recovery, and Forensics.

Figure 1. Five critical stages of cyber protection

Obviously, the goal of most IT professionals is to ensure the highest possible level of all five factors. That's not always possible, which is where resilience comes in.

Cyber resilience represents the ability to prepare for, respond to, and recover from adverse events such as cyberattacks, natural disasters, equipment and communication failures, and more.

In an ideal world, we wouldn't need resilience. But in the real world, we absolutely do. Losing resilience—or failing to create conditions that foster resilience—can have a serious impact in a number of ways:

- Employee productivity
- Loss of reputation
- Operational continuity
- Loss of business

But beyond defending your organization against attack and helping you recover in the event of a security incident, creating a comprehensive data resilience program can have immediate and long-term benefits for your organization:

- Simplifies regulatory compliance due to a clear understanding of your organization's overall posture
- Reduces the incidence and impact of adverse events thanks to a greater level of IT maturity
- Increases cost savings through reduced financial risk due to breach and loss

Let's look at how SMBs can go about building resilience for the real world.

Building Cyber Resilience

Microsoft CEO Satya Nadella announced in 2019 that "every company is a software company." Think you're not in the software business? You're probably wrong. Today, software doesn't just drive productivity in a number of areas of your business—it unites almost every department of your business through processes that are defined by and dependent on software.

What this means for you is that you can't afford not to understand the IT infrastructure that underlies your everyday business activities. And as your organization's IT matures, you'll naturally want to add layers of protection, recognizing the criticality of software to your company's products and services.

The following strategies will help grow your organization's resilience, ensuring that you can pivot optimally and recover from any type of adverse event.

Strategy #1 – Understand Your Business's Unique Needs

There's no such thing as a one-size-fits-all data protection and security strategy. No set of policies or procedures can be created that suits all businesses, since you, your activities, and your priorities are completely unique. So, it's up to you to determine, in collaboration with all departments and stakeholders, what your most vital resources and processes actually are.

Sometimes it helps to define "never events"—a term from the world of medicine that refers to events of such severity that they can never be allowed to happen. For example, it's too easy to promise "zero downtime" without the actual ability or a plan in place to make that happen and without buy-in from stakeholders across the entire organization.

That process isn't simple; indeed, it may be the most complex issue touched on in this ebook. But there are a few steps that can make it simpler.

STEPS FOR RESILIENCE

- Evaluate the types and severities of risks your business is most likely to encounter
- Ensure that you have surveyed your entire organization and documented key processes
- Conduct a risk assessment to identify vulnerabilities and analyze potential business impacts
- Document your current procedures
- Begin moving toward disaster recovery planning and testing (more on this below)

Strategy #2 – Balance Security and Protection

It is too common a mistake to assume that data protection and data security are the same thing.

While there is some overlap, this belief can lead to some faulty assumptions. For instance, if you have bulletproof cybersecurity, why bother with data protection in the form of backups? And if you have a great backup system working well, do you really have to worry about cybersecurity? Or, going one step further, if you have great backup and great cybersecurity, do you really have to worry about disaster recovery?

Well, by now, you probably know the answer to all of these questions. You absolutely need to protect both aspects of your business:

- **Data protection** keeps your valuable data backed up and available in the event of a disturbance.
- **Data security** keeps your organization up-to-date with current threat intelligence to stay safe from online threats.

To achieve the right balance of protection and security, you'll need to assess and deploy appropriate tools that prioritize your business-critical data, systems, and applications.

STEPS FOR RESILIENCE

- Implement a backup plan and test it regularly by attempting to recover from a backup
- Protect backups, for instance, by conducting backup scans for malware and air-gapping, meaning that backups are not connected to live company networks
- Adopt a security platform that provides a broad range of cyber protection across your entire environment to minimize the headache of configuration and maintenance.
- Implement a comprehensive patching program covering all OSes and endpoints in use within your environment.
- Select tools and applications that provide automation wherever possible.
- Make use of immutable storage for essential data retention, either for a fixed amount of time or permanently

Strategy #3 – Adapt to the New Normal

Cybercrime isn't the only thing that's changed over the last few years. The new normal at work is a lot more complicated through factors like BYOD, IoT, work-from-home, and a massively distributed workforce across time zones and continents.

This creates a wider range of new potential attack surfaces and methods, and old school, tool-based security strategies just aren't going to cut it. For example, a classic virus scanner or firewall won't do much good if the device being attacked is outside your local network.

Should you just use a VPN? Or go back to using agent-based security tools and platforms? The answers to these questions are complex, and may require expert advice. Yet in order to stay competitive against larger enterprises, these are essential capabilities to master – no matter the size of the business.

STEPS FOR RESILIENCE

- Gain as comprehensive an understanding as possible of your entire environment (range of endpoints, devices, etc. that require protection).
- Select a strategy to protect all endpoints while minimizing the risk of lateral attacks from within your network.
- Wherever possible, implement a zero-trust approach that limits access to confidential or sensitive data.
- Build a corporate culture of secure data access and transmission as well as risk awareness (along with an understanding of the strategic importance of cyber resilience to the business).

Strategy #4 – Don't Forget the Cloud

The cloud has been extremely good to SMBs, offering powerful business applications that scale up or down as you need, saving costs on capital expenditures (CapEx), and letting you control costs as you grow. But it's also a source of some of your greatest vulnerabilities.

Perhaps the biggest mistake most organizations make in migrating to the cloud is assuming that SaaS app providers will handle security. In fact, the risks of the cloud increase as your business activities migrate more and more to cloud-based platforms and your cloud posture becomes more complex.

Most SMBs aren't aware of the security risks of apps like Google or Microsoft cloud-based productivity and collaboration tools. For instance, many employees and end-users reuse the same password 63% of the time, across both personal and corporate accounts. And once a hacker obtains a single password, they can try it on every account they find for that individual.

STEPS FOR RESILIENCE

- Educate all users about the risks associated with common SaaS applications – especially email tools – due to the rise in social engineering/phishing attacks
- Enable multi-factor authentication for all SaaS apps wherever this isn't done automatically

Strategy #5 – Plan for Disaster

Earlier, we mentioned the old adage, "failing to plan is planning to fail." Nowhere is this truer than when it comes to the kinds of disaster situations that nobody wants to think about. While both data protection and data security are essential, as mentioned above, neither entirely covers the situation of what to do when the worst actually does happen.

For that eventuality, you need a detailed, comprehensive plan for backup, recovery, and remediation that covers all aspects of your business.

Obviously, every organization hopes they will never need to use it. But you need to view this plan as your IT insurance policy that will keep your employees, customers, and your organization's reputation safe should disaster strike.

STEPS FOR RESILIENCE

- Keep in mind the risk analysis and other business priorities identified above in Strategy #1 – "Understand Your Business's Unique Needs," including evaluating costs versus risks to create crystal-clear prioritization.
- Prepare a range of recovery methods, including offline backups or disaster recovery solutions that are inaccessible to attackers.
- Create a plan for a graceful shutdown in the event of a breach or disaster. (Don't leave customers hanging; have an incident response plan!)
- Establish a hierarchy and clear roles to ensure smooth teamwork and a cohesive, orderly approach to recovery.
- Ensure that your recovery plan includes—once the situation is resolved or remediated—a plan to reassess resilience, derive lessons learned, and implement changes based on any event that does take place.
- Test incident plans regularly (a full day once a year doesn't cut it anymore!), making testing and exercises as realistic as possible.

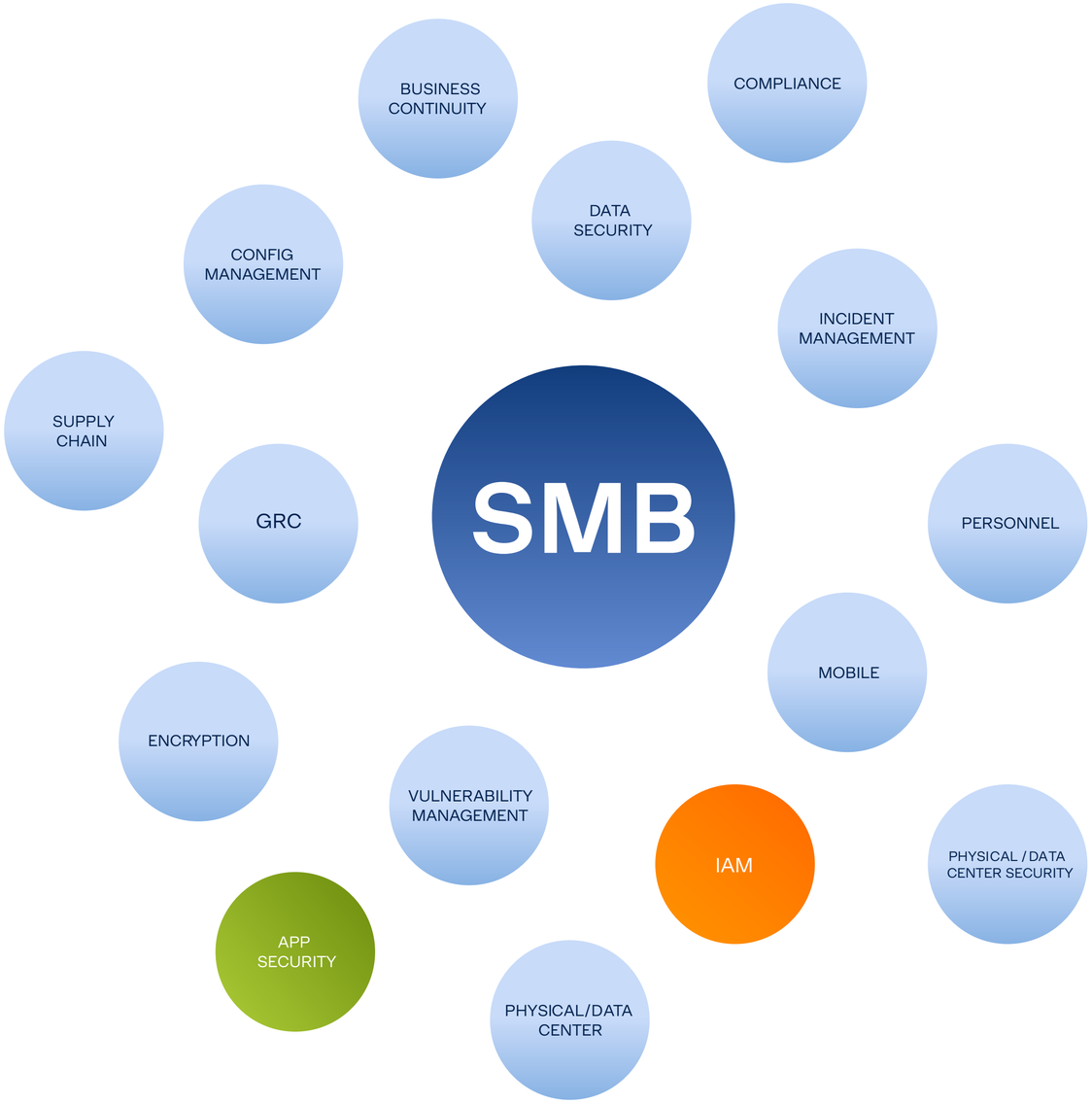
SMB Security Challenges

We've seen that SMBs lack the resources and expertise to navigate today's perilous cybersecurity waters. Just a few of the unique challenges include:

- Almost 1/3 of SMBs have had a breach within the past five years.
- More than 20% of SMB leaders have no backup or disaster recovery plan.
- Most admit they can't properly staff essential IT roles due to budget and personnel limitations.
- Over 60% of SMBs say they aren't qualified to handle security issues in-house.

Rising to meet the challenge of the unique SMB IT challenges are managed service providers (MSPs). According to TechTarget, an MSP is "a third-party company that remotely manages a customer's information technology (IT) infrastructure and end-user systems."

In theory, working with an MSP can level the playing field, letting resource-strapped SMBs outsource some or all of their IT management and security needs. Unfortunately, this clear market gap has not gone unnoticed. Today, the MSP field has been flooded with newcomers, not all of whom have the qualifications or experience required. MSPs also often have "look-alike" offerings, making it hard for customers to differentiate. Any MSP hoping to succeed must provide a broader range of offerings to help them stand out from the crowd and establish their expertise in the key domain of security.



Acronis: All-in-One Integrated Data Protection & Cybersecurity

Acronis Cyber Protect offers organizations the technology and strategies needed to build cyber resilience. Acronis Cyber Protect reduces costs, providing you with an all-in-one integrated data protection and cybersecurity solution offering:

- Built-in, proactive anti-malware, ransomware, and crypto-jacking protection
- Advanced data protection, security, management, and file sync and share
- Backup and simplified recovery

Learn more about Acronis Cyber Protect for businesses and how it enables Cyber Resilience for thousands of organizations like yours.

Acronis