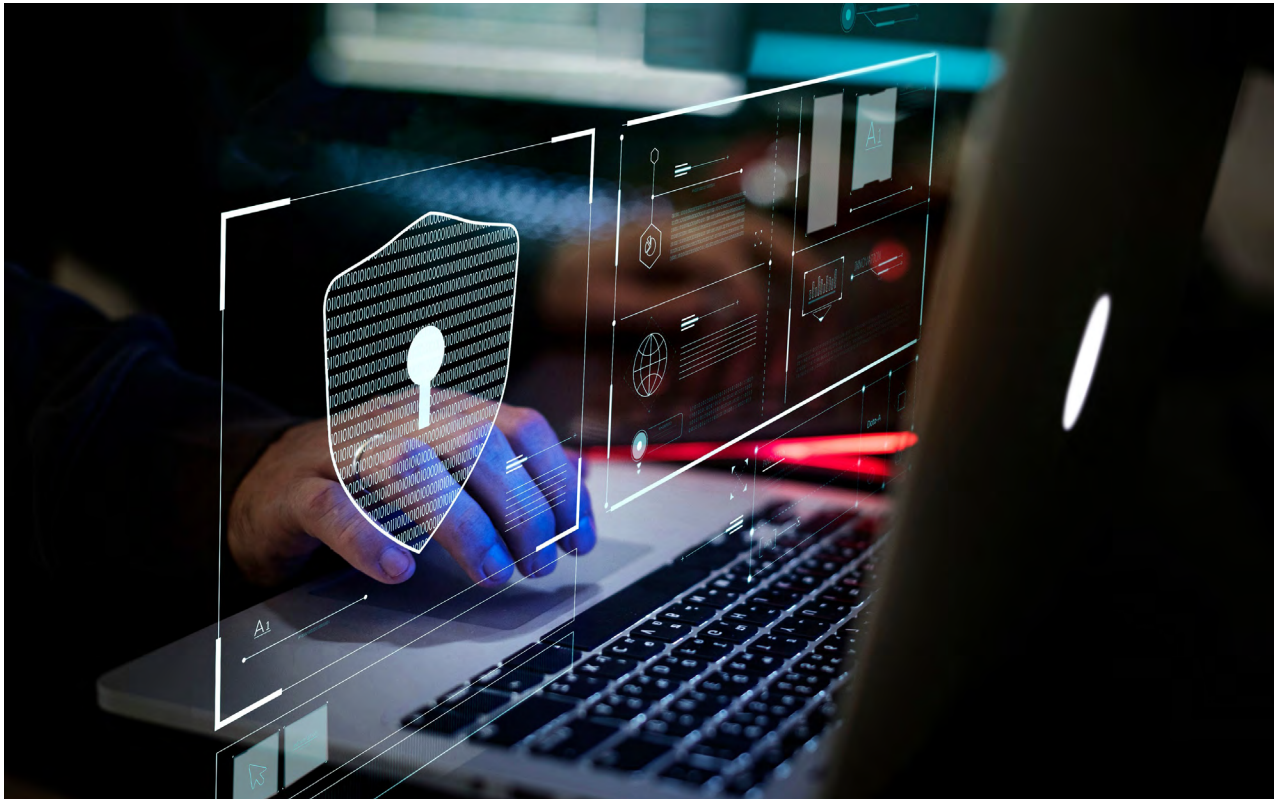


Cyberattacks on Small Businesses are Big Business.

Here's How to Avoid Becoming a Victim.

xerox™

Table of Contents

Introduction

Most small and medium businesses understand cybersecurity is a priority. But too often, it falls to the wayside in the crush of miles-long, daily to-do lists, the press of urgent client needs, unrelenting pressure from competitors, and the ever-present needs of staff.

It's easy to think that cybersecurity doesn't matter. After all, why would a hacker or bad actor target a local accounting firm, an insurance broker, real estate agent, pool repair business, or primary care clinic? Wouldn't they go after Fortune 500 companies with deep pockets and an intense desire to avoid the reputation hit of bad publicity?

That rationale makes sense if you're the good guys. But the bad guys play a volume game – routinely sweeping as many unsuspecting small business targets into the net as they can – and they're good at it. In fact, recent research from Barracuda Networks shows that "small businesses are three times more likely to be targeted by cybercriminals than larger companies."

What's more, according to a Duke University study, "85% of firms with fewer than 1,000 employees have had systems penetrated by hackers as compared to 60% of larger companies." Overall, 62% of small businesses have experienced an attack, Cisco research noted.

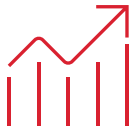
The following pages explore why cybersecurity threats are real, what makes regular businesses like yours such good targets, and how to assess and manage your risk.

Cybersecurity and Small Businesses: By the Numbers

The numbers tell a sobering story. Small and medium businesses aren't remotely beneath the notice of hackers and other bad cyber actors. In fact, just the opposite is true; their small size and comparative lack of security resources mean they present a target that's simply too tempting to resist.

Here's what we know.

IT'S INCREASINGLY LIKELY YOU'LL BE TARGETED



From **2020 to 2021** alone, cyberattacks on small businesses accelerated by

150%

RiskRecon

THERE ARE BIG CONSEQUENCES

60%

of small businesses go **out of business within six months** of a cyberattack or data breach.

Cybersecurity Ventures

RESOURCING VULNERABILITIES ARE EXTENSIVE

Small companies are, "half as likely as big companies to test their own systems, **hire data security staff, or require data security employee training**."

Duke University

LACK OF PREPARATION IS A SUBSTANTIAL WEAKNESS

66%

of small business owners do not have a cyberattack prevention plan, and two-thirds don't believe an attack is even likely.

1 in 4 say they need help knowing where to begin.

Keeper Security

TOO FEW COMPANIES ARE READY TO DEFEND THEMSELVES

Only **14%**

of U.S. small businesses are **prepared to fight** against cyberattacks.

Accenture

MANY DON'T HAVE THE INSURANCE TO PROTECT THEMSELVES

71% of so-called middle market businesses have cyber insurance – but less than 30% of small businesses have coverage (Nationwide). That's a problem; the cost of a cyberattack to small and medium businesses is

$120K on average.

Kaspersky

What's Happening and Why You?

It's easy to imagine a cybercriminal: the Hollywood stereotype of a lonely, morally compromised nerd in his basement, hacking away. The reality couldn't be further from the truth. Cybercrime is big business – in fact, one report noted that were it an economy, it would be the world's third largest (behind the U.S. and China) at $6T globally.

In short, criminals are running sophisticated enterprises and they're making incredible profits – at your expense.

HERE'S WHY YOU SHOULD BE CAUTIOUS:

1. You're easy: Small businesses don't have the same level of cybersecurity that large companies do, so an attack against you is a lower-effort, higher-reward endeavor. The cost/benefit analysis of targeting you versus a Global 2000 firm nearly always looks favorable to a cybercriminal.

2. You have sellable information: From clients' personally identifiable information like social security numbers to proprietary intellectual property, you have a treasure trove of assets waiting to be leveraged, ransomed, sold, or otherwise exploited.

3. Your people make you vulnerable: Trusting, untrained employees can be unwitting entry points to your most valuable data. In fact, "70% of entries into corporate networks come via email." Just one click on one link can open the virtual doors of your business to anyone who wants to walk through.

SO, WHAT DO YOU DO ABOUT IT?

Consider your personal health for a moment. Most of us head to the doctor well before we're actually sick. We use annual check-ups as a way to get a baseline on our health, and identify areas of opportunity to get healthier.

Cybersecurity is no different. It requires a very similar approach that begins with a methodical assessment of your own cybersecurity strength.

Seven Components of a Comprehensive Cybersecurity Assessment

A GREAT CYBERSECURITY ASSESSMENT WILL:

1. Assign a risk level based on the value of the different kinds of data you have and the importance of each system that supports your business
2. Validate each security technology you've integrated into your IT environment to make sure they're compliant and do what they're intended to do
3. Understand the efficacy of your physical security
4. Include vulnerability scans and penetration testing to see how easy it is to access your systems and data
5. Test password effectiveness
6. Examine your firewalls and wireless technology
7. Review security policies, procedures, and employee training

So, What's Next?

Once you've done a thorough cybersecurity risk evaluation, it's time to put some energy and action behind a "get well" plan. It's essentially a roadmap of steps you can take to ensure that you effectively close the gaps and raise your confidence in your systems, people, and processes.

These may include:

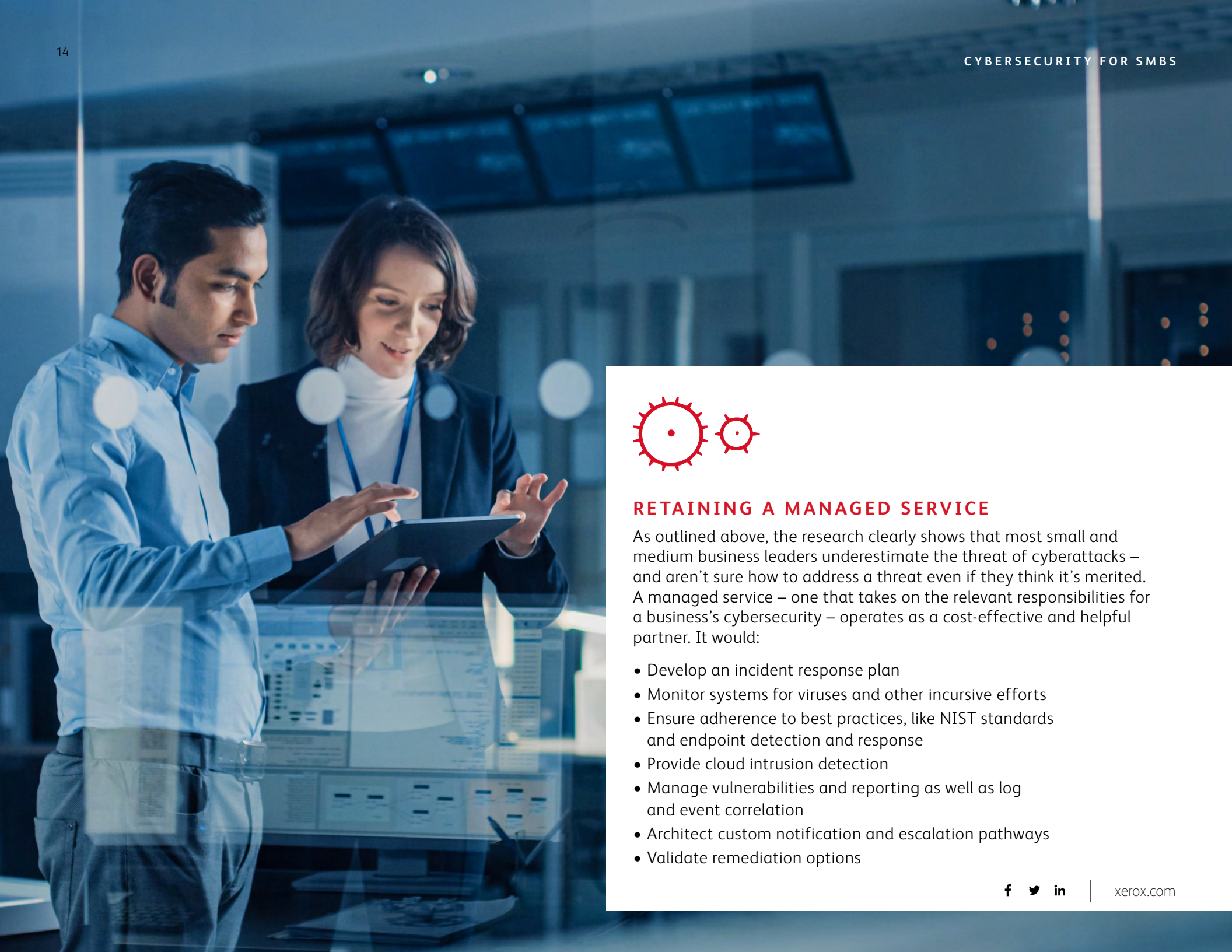
- Training employees
- Leveraging low-hanging fruit
- Retaining a managed service

TRAINING EMPLOYEES

It's surprising but, "employee mistakes and system errors are a larger threat to data security than hackers or insiders," according to TechRepublic. Regular, mandated training that teaches employees how to recognize common issues like phishing, smishing, and other social engineering techniques commonly used by bad actors can easily fill this chink in your armor. And it doesn't have to be expensive. Good security training that's engaging to take and easy for employees to remember won't actually break your bank – but will pay dividends in attacks avoided.

LEVERAGING LOW-HANGING FRUIT

Make sure multi-factor authentication is turned on for relevant employee apps. Make Virtual Private Network (VPN) access a requirement for remote employees working from home or other non-company locations. Tighten procedures and implement monitoring software for employee termination, ensuring that device and data access are turned off in a timely fashion, so there is no risk of retaliation, theft, or malicious behavior. Update policies and conduct an internal awareness campaign with employees.



RETAINING A MANAGED SERVICE

As outlined above, the research clearly shows that most small and medium business leaders underestimate the threat of cyberattacks – and aren't sure how to address a threat even if they think it's merited. A managed service – one that takes on the relevant responsibilities for a business's cybersecurity – operates as a cost-effective and helpful partner. It would:

- Develop an incident response plan
- Monitor systems for viruses and other incursive efforts
- Ensure adherence to best practices, like NIST standards and endpoint detection and response
- Provide cloud intrusion detection
- Manage vulnerabilities and reporting as well as log and event correlation
- Architect custom notification and escalation pathways
- Validate remediation options

Learn More

For any business, but especially small and medium companies, getting breached is not a question of if, but when. Xerox® IT Services includes cybersecurity experts ready to tailor best practices and insights to your unique situation and needs. Get in touch today to learn more at xerox.com/managedsecurityservice.

About Xerox

About Xerox Holdings Corporation

For more than 100 years, Xerox has continually redefined the workplace experience. Harnessing our leadership position in office and production print technology, we've expanded into software and services to sustainably power today's workforce. From the office to industrial environments, our differentiated business solutions and financial services are designed to make every day work better for clients — no matter where that work is being done. Today, Xerox scientists and engineers are continuing our legacy of innovation with disruptive technologies in digital transformation, augmented reality, robotic process automation, additive manufacturing, Industrial Internet of Things, and cleantech. Learn more at xerox.com.