By the Numbers: Why Small Businesses Have to Prioritize Cybersecurity in Order to Survive

While big companies can survive attacks using their massive financial and legal resources, many small businesses aren't as fortunate.

Perhaps that's why attackers are so eager to target small and medium-size businesses (SMBs), and why each new global crisis gives rise to a new round of attacks.

This infographic walks through the risks small businesses face and demonstrates how devastating an attack can be to a small organization's very chance of survival.

It also reveals one simple but critical step small businesses can take to protect themselves.

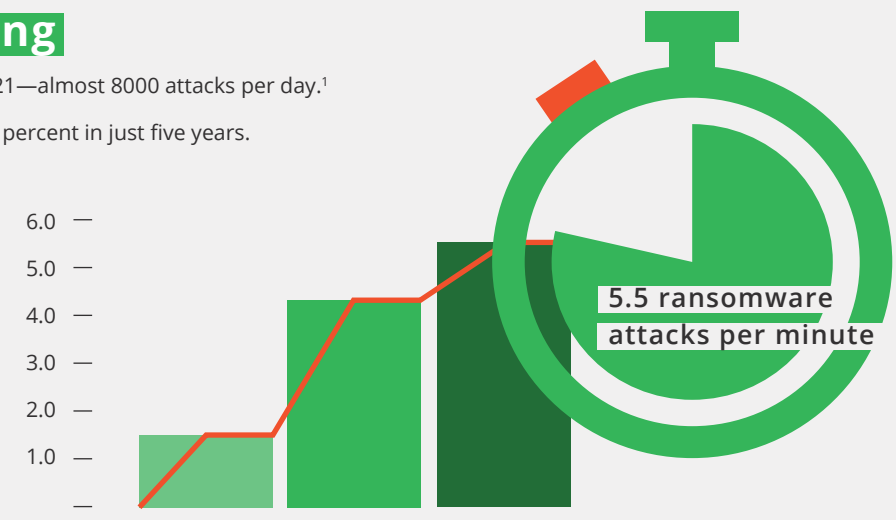
The pace of cyber attacks is increasing

Experts expect ransomware attacks to occur at a rate of 5.5 attacks per minute in 2021—almost 8000 attacks per day.[1]

That's up from 4.3 per minute in 2019 and 1.5 per minute in 2016, an increase of 267 percent in just five years.

8000

ransomware attacks per day in 2021



Attackers have big appetites for small businesses

Nearly 50 percent of all cyber attacks are committed against small businesses[2]

Small businesses are victims in more than 1 in 4 reported security breaches[3]

Owners of small businesses are more likely to pay ransoms to perpetrators of ransomware attacks than leaders of larger businesses are[4]

50%
of cyber attacks happen to small businesses

1/4
victims of security breaches are small businesses

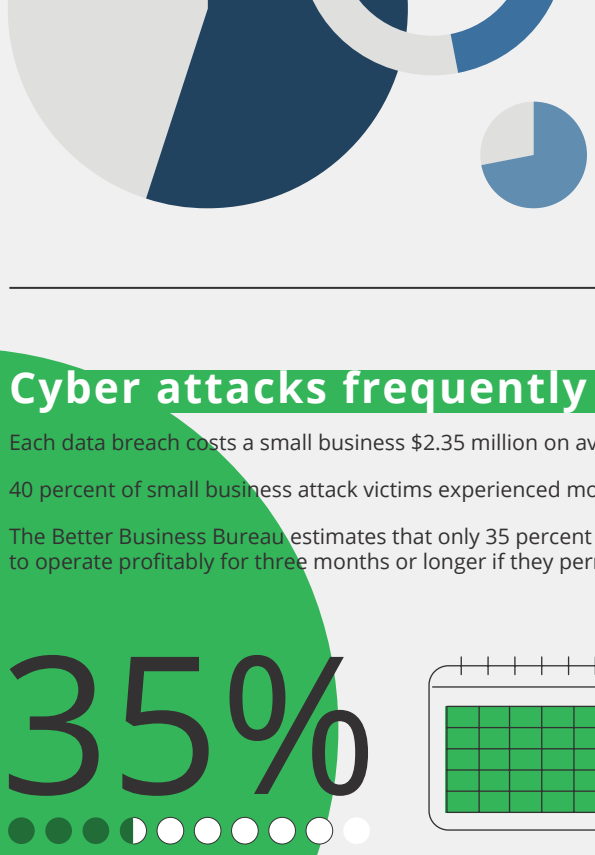
Even worse, small businesses aren't prepared for attacks

43 percent of SMB owners have no cybersecurity defense plan in place[5]

One-third of companies with 50 employees or fewer rely only on free, mostly inadequate, cybersecurity applications intended for consumers[5]

60%

of small-business owners don't think their businesses are likely targets for cyber criminals[5]



Small businesses also suffer because limited resources make them vulnerable

- The biggest challenge for 55 percent of small businesses in developing a cybersecurity plan is lack of resources or knowledge[6]
- 47 percent of respondents to one survey say they have no understanding of how to protect their companies against cyber attack[7]
- 72 percent of respondents to the same survey said that malware—essentially files that launch attacks—has slipped past their systems for intrusion detection[8]

Cyber attacks frequently cripple and kill small businesses

Each data breach costs a small business $2.35 million on average[9]

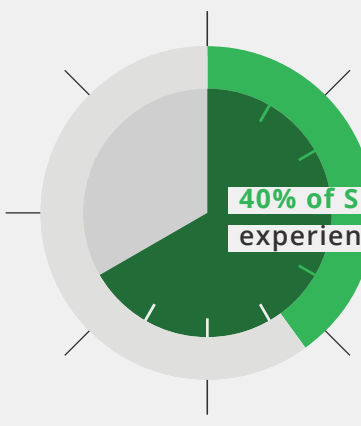
40 percent of small business attack victims experienced more than 8 hours of downtime[10]

The Better Business Bureau estimates that only 35 percent of small businesses could continue to operate profitably for three months or longer if they permanently lost data due to an attack[11]

$2.35
million
the average cost of a data breach on a small business

35%

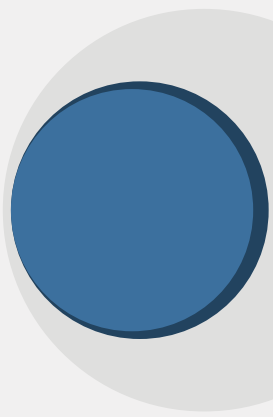
of small businesses could continue to operate profitably for 3+ months if they permanently lost data due to an attack



40% of SMB attack victims
experience 8+ hours of downtime

And the bottom line...

60 percent of companies that suffer a cyber attack are out of business within six months[12]



Damage done by attacks goes beyond financial losses

64% percent of customers said they would **cease to work with a company** if their personal or financial information were stolen[13]

94% of those customers would consider taking **legal action** against the hacked company[13]

Small businesses can make cybersecurity a priority even with limited resources

Obviously, antivirus systems are a must for all businesses, and there are other applications that can protect email and guard against attacks. But some attacks can fool even the best protection systems. The average time to identify and contain a data breach is a whopping 280 days.[14]

When small businesses move accounting and associated critical business applications to the cloud and trust the operation of their software environments to a cloud provider, they provide employees real-time access from anywhere and ensure that people can work from wherever they are.

But they do much more than that. They minimize the threat of attacks by turning security over to experts who can save them from disaster.

As a cloud provider, Right Networks can actually detect threats that antivirus and other security systems don't yet recognize and neutralize those threats without causing any downtime for the business. So, those eight hours or more of downtime that so many businesses suffer becomes a total non-event when an attacker attempts to damage a business.

Moving accounting and business applications to the cloud enables small businesses to protect profitability, minimize threats and ultimately stay in business. It's the first and most effective measure businesses should consider when prioritizing cybersecurity.

Sources

[1] https://www.accountingtoday.com/news/cybersecurity-staying-vigilant-and-safe
[2] https://www.entrepreneur.com/article/301193
[3] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[4] https://www.cisco.com/c/dam/global/hr_hr/solutions/small-business/pdf/small-mighty-threat.pdf
[5] https://www.prweb.com/releases/new_study_reveals_one_in_three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm
[6] https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf
[7] https://www.keepersecurity.com/ponemon2020.html
[8] https://www.keepersecurity.com/ponemon2020.html
[9] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf
[10] https://www.cisco.com/c/dam/global/hr_hr/solutions/small-business/pdf/small-mighty-threat.pdf
[11] https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf
[12] https://www.fundera.com/resources/small-business-cyber-security-statistics
[13] https://www.cpapracticeadvisor.com/firm-management/article/21122106/why-preventing-data-breaches-should-be-a-top-priority-for-cpa-firms
[14] https://www.fundera.com/resources/small-business-cyber-security-statistics