cyberconIQ

White Paper

Keeping Small & Medium-Sized Businesses Safer Online

Dr. James Norrie, April 2022

What Can Actually Keep SMB's Safer Online?

Solving the Cybersecurity Challenges of Small Businesses

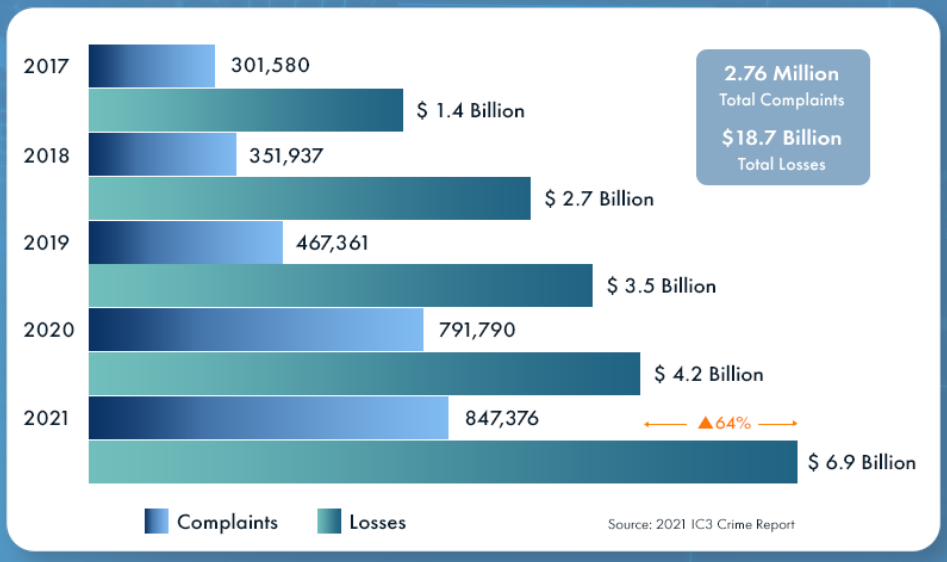
The Online Threat to Small Business Is Real

What is clear now is that businesses of all sizes are at risk of becoming cybercrime victims. No business is immune, and the threat of being hacked is not a function of the size of your business. Don't fool yourself – they are coming for you.

And this is a function of geography mainly. North American businesses are attacked more frequently than anywhere else. Why? Because we enjoy a stable, capital and technology-enabled business environment supported by globally traded currencies that make us attractive targets for overseas crime gangs to exploit.

How do we know this? The crime data tells the story, starting with the annual report from the Internet Crime Reporting Center (IC3) which is operated by the FBI in the United States. Generally, most cybercrime goes unreported for lots of reasons including that law enforcement is overwhelmed and cannot provide much immediate help to online victims of cybercrime. That crime also often originates overseas so it is impossible to pursue and solve. Or the embarrassment and shame of having been a victim of a preventable crime means you just accept having been victimized and move on instead of reporting the crime. Regardless, anyone can clearly see the trend in this data. It's rising every year.

Cyber Crime Complaints & Losses over Five Years



Three Pillars of Defense for Small Business

1 Continuous Monitoring

2 Making Employees Your Human Firewall

3 Extended Services Warranty

Pillar 1: Continuous Monitoring

Most small businesses do not have a dedicated IT team of their own, or they have limited internal IT resources often without cybersecurity expertise. But that should NOT stop you from deploying simple outsourced IT solutions that can prevent many attacks even before they get started. Like a burglar alarm system for your home, this cybersecurity early warning system is monitored 7/24 on your behalf and our experts look for the signs of danger and either repel them before they can enter your business systems or even shut your systems down to prevent further damage until experts can remediate your systems safely.

Either way, an ounce of prevention is worth a pound of cure as they say, and this simple and cost-effective solution is a fast pathway to making your business systems more secure. Of course, **no technology can prevent 100% of attacks** and technology can only detect known attacks. So that brings us to your next line of defense.

Three Pillars of Defense for Small Business

Pillar 2: Making Employees Your Own Human Firewall

Hackers target your employees every single hour of every single day looking for vulnerabilities they can exploit. These include **phishing, smishing and vishing attacks** designed to deliver either ransomware or malware into your business in just a single quick click. Or wire transfer and man in the middle attacks to deviate payments to crooks. Business email compromise, credential hacking and social engineering designed to steal your data. All of these methods intend to make a loyal, hard working employee a vector of attack so they compromise your systems from the inside out. We call this an accidental insider - somehow who is manipulated into causing a breach without meaning to.

Today, these kinds of attacks represent between **56% - 90%** of all successful online attacks against small businesses. And NO technology can prevent these attacks because they involve a human being duped to compromise the technology.

What is the best line of defense against these kinds of attacks? Train every single one of your employees on how to spot them, prevent them and report them BEFORE they click.

At cyberconIQ, we make your company more secure one employee, one style and one lesson at a time. Learn more about our entirely online, inexpensive, and **highly effective security training platform that can keep anyone safer online**.

Three Pillars of Defense for Small Business

1 Continuous Monitoring

2 Making Employees Your Human Firewall

3 Extended Services Warranty

Pillar 3: Extended Services Warranty

We are confident our bundled cybersecurity services offer small businesses easy access to basic solutions they need at an affordable monthly rate that will pleasantly surprise you and significantly reduce risk of a successful cybersecurity attack on your business.

Yet, nobody can ever guarantee they can prevent every single kind of cybersecurity attack. And the costs of remediating and reporting a successful attack can cause you to lose your business. In fact a recent **Inc.** magazine study found that **60% of small businesses that suffer a successful cybersecurity breach will go bankrupt within six months** due to the costs of reporting, remediating and restoring their business technology after an attack. This is a sad reality that our extended warranty plan can address by providing tiers of coverage geared to paying for the direct costs of a breach if one were to occur.

Because cybersecurity insurance is both expensive and sometimes hard for small businesses to obtain, if you subscribe to one or more of our services then we can provide a warranty that will help protect your business from overwhelming costs if you are successfully breached.

If you are ready to learn more about how we can help you protect your small business from cybersecurity attacks, contact us today at info@cyberconIQ.com or call us at 1-833-888-0392!

Why Engage With Us?

We promise that the information you will receive will be valuable and independent of your decision to explore a business relationship with us. As experts in behavioral science, often called upon to advise clients on improving their security program maturity, we know how to **reduce cybersecurity risk, everywhere and every time**. While our platform makes all of this easy, our goal is always to deliver critical insights that help everyone stay safer online. We are here to help.

Learn more at **cyberconIQ.com**.

Data Breach Statistics for 2021

Ransomware Still on the Rise

Appearing in **10%** of breaches - more than **double** from 2020.

The Human Element

85% of breaches involve the human element. Breaches caused by **phishing** were also up **25%**.

Business Email Compromise

The **second-most common** form of social engineering leading to a cyber breach.

*Source: Verizon DBIR, 2021 Data Breach Investigations Report - https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf