NO ONE WANTS TO HACK MY BUSINESS

YOU'RE WRONG.

THEY DO – ESPECIALLY IF YOU'RE AN EASY TARGET
(AND YOU PROBABLY ARE).

IF YOU'RE A SMALL OR MID-SIZED BUSINESS OWNER,

you may not know why your business would ever be targeted by hackers. After all, your business probably doesn't handle nearly as much money or personal information as larger companies do.

While that's true, most large companies are aware that they're major hacking targets. They have the money to invest in cutting-edge cybersecurity, and they do so.

Hacking a single small or mid-size business won't produce a lot of money or personal information for a hacker. However, it's much easier. Small businesses are low-hanging fruit, compared to larger organizations, and hacking a few small businesses successfully is far more profitable than trying to hack a major company.

And let's be clear about this – hackers are criminals. All they want is money. Easy money. They don't care who they steal from – and SMBs are often easy money.

Protect yourself or their next victim could be you.

YOU COULD BE NEXT

61% of data breach victims were businesses with fewer than 1,000 employees.

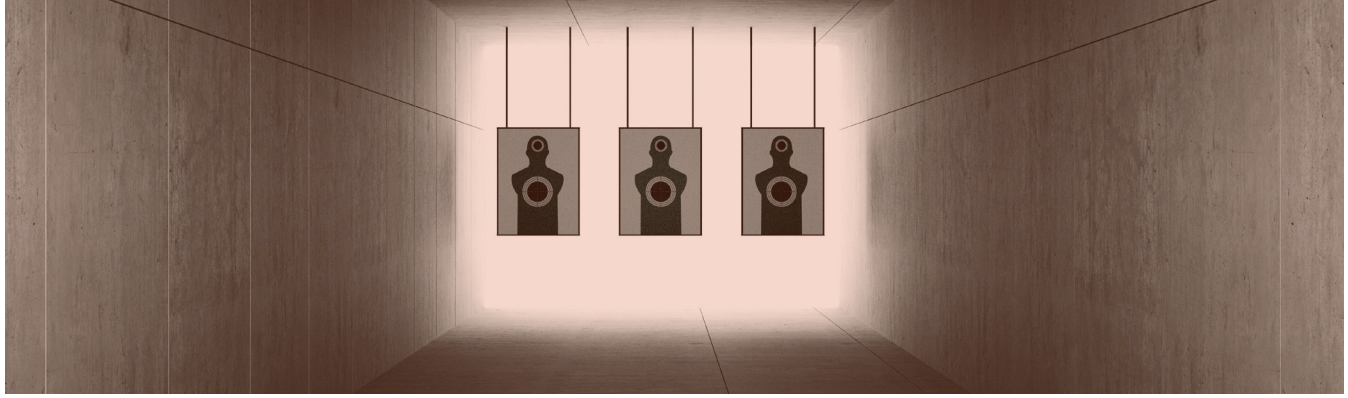
Cybercriminals don't just target large companies.

In the following pages, we're going to convince you that you need to take information and network security seriously.

Because if you don't, there's a good chance you won't stay in business if your security is ever breached.

Some of you reading this probably think this all sounds like hyperbole and it'll never happen to you. Who knows, you might get lucky. We're in Las Vegas, maybe you think you'll keep rolling sevens or drawing inside straights.

BUT WHAT ARE THE ODDS OF THAT?



SMBS ARE VULNERABLE AND TARGETED

1

- Last year alone, 63% of small businesses in the USA said they had been attacked at least once.

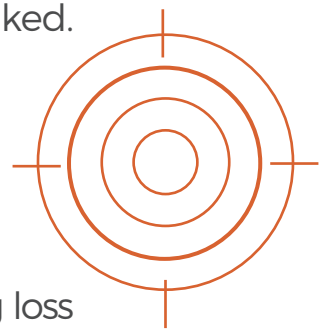
- A Towergate survey notes that 82% of affected small business owners assumed they had nothing worth hacking or stealing, so their network security was weak or entirely missing.

- Small businesses often don't recognize the value of data and fail to put up a proper defense.

REALLY, SMBS ARE VULNERABLE AND TARGETED

31% of targeted attacks focus on businesses with fewer than 250 employees
(Source: Symantec)

This year, 40% of small to medium sized businesses that manage their own network and use the Internet for more than email will have their network accessed by a hacker, and more than 50% won't even know they were attacked.
(Source: Gartner Group)



20% of all small businesses will be hacked within one year.
(Source: National Cyber Security Alliance)

20% of small to medium sized businesses will suffer a major disaster causing loss of critical data every 5 years.
(Source: Richmond House Group)

THE THREAT IS GROWING

Symantec research shows that in 2016, 101 new families of ransomware were discovered. The majority of attacks still occur against individuals; mostly because after a spike in attacks on business, businesses began protecting themselves against ransomware.

That said, Symantec research indicates that cybercriminals will target more businesses with ransomware because that's where the money is, "while ransomware attacks to date have been largely indiscriminate, there is evidence that attackers have a growing interest in hitting businesses with targeted attacks."

ANYTHING WITH A HARD DRIVE OR CONNECTED TO THE INTERNET CAN BE HACKED

Too many business owners think only of their computers when it comes to security. Broaden your perspective: anything with a hard drive is a potential security hole – digital copiers, printers, tablets, smart phones. Make sure they're included in your security policy or you may as well not have one.

And we mean ANYTHING connected to the Internet. Security breaches have occurred through climate controls and through teddy bears. CloudPets toys had 820,000 user profiles exposed.

NIGERIANS STILL IN BUSINESS

We laugh at the obviousness of it – I'm in Nigeria and have just received a large inheritance, but I need to put the money in your banking account to have access to it. Please give me your banking information in exchange for a cut of the money.

But phishing emails work. 1 in 14 users in 2016 were tricked into following a link or opening an attachment.

In 2016, one of every 131 emails sent were malicious – the highest rate in five years.

YOU ARE A TARGET.
PROTECT YOURSELF!
YES, WE ARE YELLING AT YOU.
IT'S THAT IMPORTANT.

CLICK HERE TO SHARE →

SECURITY BREACHES AREN'T JUST ANNOYING

Sure, it's annoying to have to rebuild your computer after a virus infection. A slight dip in productivity is the least cost possible.

A breach due to insufficient network security can also result in the loss of critical data, which could jeopardize operations on many levels. Partners or clients who do not trust that their data is secure in your hands will do business elsewhere. Both of these long-term consequences of getting hacked could have you reeling financially, but losing the trust of your big clients is something you might never recover from.

DATA BREACHES COST MONEY

Costs per breach are up.

$221 average cost per compromised record is the highest since the first report 11 years ago.

Indirect costs are $145 of this – including abnormal turnover and customer churn.

Regulated industries have higher data breach costs. The cost per breach for healthcare ($402), life sciences ($301), and financial services ($264) is higher than the average.

LOST BUSINESS COSTS YOU MONEY

Lost business costs are rising.

After a spike to a loss of $4.54 million in 2011, costs from lost business dropped to $3.01 million in 2012. However, they've steadily risen yearly to $3.97 million in 2016.

A BREACH COULD KILL YOUR BUSINESS

93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster. (Source: National Archives & Records Administration in Washington DC.)

Looking for ROI for an investment in network security? There's no greater return than avoiding an "Out of Business" sign.

THERE'S NO SUCH THING AS 100% SECURITY

Security threats change weekly. There's always a race on between security pros and cybercriminals. Unfortunately, sometimes the cybercriminals are ahead in the race.

Plus, new technology always creates new security concerns – email, PDAs (and now smartphones), cloud business apps and storage. These technologies and others have all created new security holes for hackers to penetrate.

Right now someone is creating some new technology "thing" that we'll all love and will drive network security professionals nuts for a while because we'll use it at work without permission or worry about security. Security is a constant, never-ending battle – don't ever think you're "finished."

YOU NEED A SECURITY POLICY

Security is too important to wing it. If you need to comply with government regulations, such as HIPAA, a security policy is a must to be in compliance. A policy is useless unless you abide by it.

You also need to update your policy as new technology becomes available. And inform your employees about the policy, update them as necessary, and provide any training needed to ensure they adhere to it.

If you think you're covered because you have anti-virus software on your computers, that's NOT a security policy.

LOOKING FOR SECURITY TIPS?

Download our 53 Timeless Information Security Tips for SMBs (And Anyone Else)

Are You Ready to Take Security Seriously?
Do you have the time and expertise to manage your security infrastructure internally?

>> CLICK HERE TO CONTACT US TODAY <<
to schedule your no obligation (and free) IT assessment.

ABOUT AIS

AIS is all about you, our customer (or potential customer – hello!).

Founded on the premise of providing excellent customer service and business solutions that work, AIS has steadily grown from our HQ location of Las Vegas, NV to four additional locations in southern California: Riverside, Palm Desert, and San Diego.

We provide copiers, printers, managed IT services, document and process management, copier and printer repair and maintenance contracts, telephone services, and are an authorized dealer of 3D Systems' 3D printer lineup.

AIS is proud of our employees, our culture, and our commitment to service. We are grateful to all of our wonderful customers.

AIS
ONE COMPANY, MANY SOLUTIONS

SOURCES

2017 Data Breach Investigation Report by Verizon
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Symantec Internet Security Threat Report, Volume 22