Small Business TRENDS
The magazine for successful small business owners

CYBER ATTACKS AGAINST YOUR BUSINESS
EVALUATE THE RISK AND PLAN YOUR DEFENSE

7 Biggest Cyber Threats to Your Small Business
How to Defend Against Cyber Attacks
Can You Recognize a Phishing Email?
Password Policy Best Practices

Spotlight:
Strongarm Protecting Small Business from Cyber Threats
Has Your Printer Been Hacked?
The Most Effective Ways to Protect Your Small Business from Cyber Attacks
The Most Effective Ways To Protect Your Small Business From Cyber Attacks

7 Types of Cyber Attacks Are Threatening Your Small Business Right Now
If you’re the owner of one of the estimated 28 million small businesses in America, you need to include cyber security as an important part of your business toolkit.
17 11 Cyber Security Questions Every Small Business Should Ask
Don’t regard a cyber attack as a potential risk for your small business? Think again. Cyber crime is on the rise and hackers are increasingly targeting small businesses.

20 Defeating Cyber Attacks on Your Business Will Require Humans and Automation
To defeat cyber crime, humans and robots are going to have to learn to work together.

23 Follow These 20 Password Policy Best Practices to Keep Your Company Secure
The Verizon Data Breach Investigations Report for 2016 tells us 63 percent of small business hackers take advantage of weak passwords.

27 10 Things Your Small Business Data Breach Response Plan Must Have
The 2016 State of SMB Cybersecurity Report from cybersecurity software company Keeper found hackers have breached half of the 28 million small businesses in the U.S.

30 97% of Your Employees May Not Be Able to Identify a Phishing Email
When you think of cyber attacks, you may imagine complex campaigns against major corporations and governments.

32 Does Your Small Business Need Data Breach Insurance?
Cyber security breaches cost businesses billions of dollars each year. Breaches in 2016 reached a record peak.

35 Data Breaches of eCommerce Retailers Cost $172 Per Record
If your small business hasn’t been “hacked,” it can be difficult to quantify the potential impact of cyber crime.

37 Is Your Office Equipment Cyber Safe? New Ratings Standard Rates IoT Products
More of the things we use in business and life are now connected.

39 Strongarm Protects Small Businesses from Cyber Threats
You’ve no doubt heard about some of the cyber attacks that have impacted large businesses and even governments in recent years.
Cyber Security Edition 2017

Cyber security and how it relates to your small business may be the topic of 2017. You read every day about security breaches and hacks but rarely do you hear about them hacking small businesses.

So that must mean the threat isn't real. These are all scare tactics.

Not so!

In fact, hackers are targeting small businesses more and more. It's because they're more vulnerable and less likely to be protected from a cyber attack.

A new study from Nationwide actually found that 76% of small business owners didn't believe their company was vulnerable to an attack. Yet, at the same time, 45% had already been victimized but weren't aware it happened.

This is why we created this Cyber Security edition of Small Business Trends magazine. We wanted to take the veil of mystery off this relatively new and unknown subject for small businesses.

In this edition, we run the gamut of cyber security. Our goal is to get you as prepared in the event of a cyber attack as possible.

The most important thing for you to realize is the risk your company faces. The risk will determine how you should combat cyber criminals. Our cover story by Michael Guta goes over that in plain detail.

Staff Writer Rob Starr discusses the 7 types of cyber attacks your small business could fall victim to and expert contributor Jeff Charles has advice on ways to protect your company from a hack attempt.

That's not all, by a long stretch.

Inside, you'll also find some password best practices. That's one thing every small business can do – for free – to protect against cyber attacks.

Plus, we've got advice on whether or not your company actually needs cyber attack insurance and how to protect devices connected to the Internet of Things.

There's all that and even more in this chock full Cyber Security edition of Small Business Trends magazine.

Wishing you much success,

Anita

P.S. Please subscribe (free) so you never miss future editions. Go to http://smallbiztrends.com/magazine.
Cyber Security Editor’s Notes

They’re From the Government and Here to Help -- No, Really

Lawmakers in Washington, D.C., are currently debating the fate of the Main Street Cybersecurity Act. There’s actually very little debate and the bill should pass ... eventually.

A version of the Main Street Cybersecurity Act has already passed the Senate. And the House of Representatives should pass their version soon.

The bill would require the National Institute for Standards and Technology (NIST) to adapt its current cyber security framework in place to small businesses and their specific needs.

Avast Offers Small Businesses Cyber Protection

Avast is utilizing its recent acquisition of AVG and putting it to good use for small businesses.

When the company acquired AVG not long ago, it also acquired additional technologies that allow it to now offer real-time cyber threat protection.

New Study Finds Small Businesses Unaware of Cyber Attacks

That kind of monitoring may be necessary because a new survey from Nationwide finds that nearly half (45%) of small businesses have been victimized by a cyber attack but were completely unaware.

That’s not the only area where many small businesses are failing to keep up to speed. Nationwide also found that 76% of small businesses believe that a cyber attack wouldn’t affect their company.

iPhone X and iPhone 8 Focus on Security

Everyone’s always excited about a new iPhone. To dampen that mood a bit, a smartphone is one area where small businesses are particularly vulnerable to attack.

Apple is addressing security, in general, with its latest iPhone releases, the anniversary X edition and the new iPhone 8. There’s no telling what could happen if your smartphone falls into the wrong hands but security features -- like facial recognition -- will make it more difficult for your device to serve any purpose for a thief.

Don’t Forget Printers -- You Can Be Hacked There, Too

Small businesses can also be hacked via the Internet of Things. It’s often these devices that lack the type of cyber security you’re likely to dedicate to your computer, laptop, or even your smartphone. But HP has just released new printers that take the issue of cyber security seriously. The company is even addressing cloud and remote printing with its HP Roam and HP Connection Inspector security features.

Shawn Hessinger
Executive Editor
@Shawn_Hessinger
Understand Your Risk, Then Invest in Your Small Business Cybersecurity Plan
Do you know the cost/benefit breakdown of the cybersecurity you have in place for your small business?

To be more precise, how much should you invest in cybersecurity protection in relation to your actual monetary risk? The findings of the new report from the Better Business Bureau, titled, “The State of Small Business Cybersecurity in North America” offers some hints.

The report was released as part of National Cybersecurity Awareness Month. And one of the more distressing data points regarding small businesses indicates half of them could only stay profitable for about a month after losing critical data.

The BBB surveyed around 1,100 businesses in the U.S., Canada, and Mexico with 71.4, 28.5, and 0.1 percent of the respondents coming respectively from those countries.

Profitability is the ultimate test of risk. It’s alarming to think that half of small businesses could be at that much risk just a short time after a cybersecurity incident.”

How Much Are Small Businesses Losing?

According to the report, the annual average loss from cyber attacks is estimated at $79,841. The median loss came in at $2,000, with the maximum total loss at $1 million. This, of course, will vary greatly with the size of your company and the type of cyberattack you have sustained.

Still Bill Fanelli, CISSP, chief security officer for the Council of Better Business Bureaus and co-author of the report, emphasized the vulnerability of many small businesses. “Profitability is the ultimate test of risk. It’s alarming to think that half of small businesses could be at that much risk just a short time after a cybersecurity incident,” Fanelli said.

It doesn’t do any good for a small business to adopt a $10,000 solution if the potential risk reduction is only worth $5,000.

Do You Know How Much to Spend on Cybersecurity?

Fanelli still stresses small businesses must avoid going overboard. He explains “It doesn’t do any good for a small business to adopt a $10,000 solution if the potential risk reduction is only worth $5,000.”

With that in mind, the report used a formula created by two professors at the University of Maryland, Martin P. Loeb and Lawrence A. Gordon. Using this formula, a small business owner can calculate the best possible investment in prevention to safeguard their company from cybersecurity attacks.

The five step process begins by estimating the loss; estimating risks; identifying investments; estimating savings; and making the calculation. You can get details of the formula on the free download of the report here.

The report adds, “As long as the potential savings exceeds the cost of investment, then it is a cost-effective measure that should be implemented.”
WOMEN IN CLOUD INAUGURAL SUMMIT
Join Us and Invest in Your Success!

Empowering Female Tech Entrepreneurship with Cloud Computing

We bring together the voices and insights of diverse female luminaries in technology, business, and government through keynote presentations, panel discussions, spotlights, and one-on-one interactions.

GET INSPIRED | GET CONNECTED | GET TO CLOUD

Speakers
Gavriella Schuster, Gretchen O’Hara, Carrie Francey and more

Location
Microsoft Building 33, 16070 Northeast 36th Way, Redmond, WA 98052, United States

JOIN US!
19 JAN 2018
9:00 AM TO 11:30 AM

SPONSORS & PARTNERS

SPONSORSHIP OPPORTUNITIES

For sponsorship inquiries, please reach out to Chaitra Vedullapalli at chai@meylah.com

Sponsorship Opportunities closes January 5th

Follow us
www.womenincloud.com
www.facebook.com/womenincloud/
The Most Effective Ways to Protect Your Small Business from Cyber Attacks

Okay, I’m going to start with a question.

What would happen if a hacker decided to launch a cyber attack against your business? Would they be successful? Would they easily gain access to your company’s sensitive information? Or would their attempt fall flat?

Believe it or not, cyber security isn’t just a concern for large businesses. It’s something that small business owners need to pay attention to.

Consider these statistics about Small Business Security:

• 43 percent of cyber attacks target small business.
• Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.
• 60 percent of small companies go out of business within six months of a cyber attack.
• 48 percent of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

If you’re a small business owner, you can’t ignore these statistics. You don’t want your business to suffer because you didn’t take the appropriate steps to protect it.

You have worked way too hard to allow your company to be threatened by a hacker, right? In this post, you will learn why it’s important to focus on cyber security. You will also learn how you can protect your business.

Why Should Small Businesses Be Concerned With Cyber Security?

I know what you’re thinking. You’re thinking that your business is so small, nobody would ever want to hack it.

It’s easy to think that a small business would never have to deal with cyber security issues. Makes sense, right? Usually when you hear about a company being hacked, it’s a major brand like Target or Sony.

But these aren’t the only targets.

It may sound hard to believe, but hackers target small businesses too. You just don’t hear about it because the media isn’t going to report on hacks involving small businesses. There are several reasons why a hacker might go after a small business...

Small Businesses Don’t Take Cyber Security Seriously

Let’s face it. Most small business owners don’t take cyber security seriously. They think that they’re too small to get a hacker’s attention.

However, this is one of the main reasons why a small business might get hacked. Hackers know that most small business owners don’t invest in cyber security.

Why? Because small business owners tend to think they have nothing worth stealing. This makes them an easy target.

Chances are, you do have something that hackers want: customer payment information. That brings me to my next point...

If you’re a small business owner, you need to take your cyber security seriously.

You Have Information That Hackers Want

Your business may not be as big as Target or Starbucks... but it doesn’t matter. You do take payment for your products and services, right? That means you have something that hackers want. You have your customers’ payment information. You have your employees’ information.

The Council of Better Business Bureaus found that 7.4 percent of small business owners have been defrauded. As a business owner, you have customer and employee information. This information is as valuable as gold to hackers. If your system isn’t secure, these hackers could have access to payment information and social security numbers. It’s your job to make sure that this information is protected.

How to Protect Your Small Business Against a Cyber Attack

Okay, so I’ve showed you that being a small business doesn’t necessarily mean that you can’t get hacked. But if you’re smart — and I know you are — you’re probably wondering how you can protect your company’s information.
Get Cyber Security Insurance

Insurance! It’s not just for your car, house or medical bills. You can also get insurance for your business. As a matter of fact, every company should carry some type of business insurance.

But, there is also cyber security insurance. If you’re a small business, you need this.

Sure, we all hope that security breaches won’t happen. But hope isn’t good enough. You need to make sure your business is covered.

Cyber liability insurance is designed to protect your business from various cyber security threats. If there is a security breach, and your company is held liable, you may end up having to pay out tons of money in a lawsuit. This can cripple most small businesses.

If you have cyber liability insurance, you won’t have to worry about this. If you buy the right type of insurance, your legal costs will be covered.

Develop a Password Strategy

Many cyber security attacks happen because the passwords your employees use are way too simple. If your team isn’t educated, it’s possible that they’re using passwords that are way too easy to hack.

It happens all the time.

That’s why you need to implement an effective password strategy. You may not be able to stop every single attack, but you can certainly slow down a persistent hacker. If your system isn’t easy to hack, it could discourage the attacker. They will move on to another small business owner who isn’t as smart as you are!

Fortunately, this is pretty easy.

You should make sure that your team members are required to create passwords that include a combination of uppercase and lowercase letters, along with numbers and symbols. Yes, I know this might be a pain, but the security your company will have is worth it. Also, you should require your employees to reset their passwords at least once a month.

Use Virtual Data Rooms (VDR)

Virtual data rooms are a great way to keep your company’s information secure. They make it easier for your employees to share sensitive data.

A virtual data room is an online repository where your company can store data. They’re usually used with financial transactions. It’s very hard for a hacker to get to information that is stored in a VDR.

There are many types of information that a company might store in a VDR:

• Financial information
• Legal documentation
• Tax paperwork
• Intellectual property information

VDR’s are a great way to ensure that your sensitive information is being kept safe.
Speak With an Expert

Yes, I know you don’t want to do it. But you should. Paying an IT security consultant might seem to be a little expensive. But it’s a great investment.

If your house sprung a leak and water was building up in your kitchen, would you try to fix it yourself? Probably not. You would probably call a plumber, right?

Why? Because if you’re like most of us, you don’t know the first thing about plumbing. The same principle applies to IT security.

If you’re concerned about cyber security, you should consider speaking with an IT security expert. An IT security consultant can take a look at your business and determine the best course of action when it comes to protecting it from cyber attacks.

An IT security consultant can identify areas where your company is vulnerable to cyber attacks. They can make recommendations that will help you keep your business safe. When it comes to cyber security, you can never be too careful. If it’s in your budget, hire an expert. You’ll be glad you did.

Beware of Internal Threats

This may be a surprise, but most of the cyber security issues that happen are the result of someone inside the company. It’s not something most business owners want to think about, but it’s totally true.

Here’s a hard truth: 55 percent of all cyber attacks come from inside the organization. 31.5 percent are done by malicious employees. 23.5 percent are done by company insiders who mistakenly leave the company vulnerable to an attack.

Protecting your company means looking within the organization. It’s easy to assume that a cyber attack is going to come from an outside force. But it’s not true. You have to focus on the people inside your company just as much as people outside your company.

The key is to find the balance between being safe and being big brother.

Make sure that you are keeping an eye on your authorization requirements. Be careful when you’re deciding which employees should have access to sensitive data. This will help you prevent “internal hacks.”

Don’t feel guilty for watching your employees’ activities; as the owner of your business, it’s your duty to ensure that you and your team are being protected. I get it. You don’t want to micromanage. The key is to find the balance between being safe and being big brother. It’s different for every company, but if you work at it, you will find that balance.

Summing It All Up

If you’re a small business owner, you need to take your cyber security seriously. Don’t assume that your company isn’t a target just because you’re not a big business.

You owe it to yourself, your employees and your customers to make sure that your business is secure. Preventing cyber attacks should be one of your top priorities. If you take the right steps, you won’t have to worry about endangering your business.
Products / Resources

Employee Vacation Tracking Template
Track vacation, sick leave, and personal leave accrual. A great tool for HR personnel.

1:1 Free Consultation To Become Microsoft Cloud Ready Partner
Is Your Company Noticed By Microsoft? Evaluate Cloud Readiness for Microsoft Partnership Request 1:1 Free Consultation ($500 value)

34 Productivity Templates Every Business Needs
34 Productivity Templates Every Business Needs: Purchase your bundle today!

Ignite Your Travels With Wholesale Travel Discounts
Ignite Your Travels With Wholesale Travel Discounts. Save Up To 70% On Your Travel.
If you’re the owner of one of the estimated 28 million small businesses in America, you need to include cyber security as an important part of your business toolkit. Almost half (43 percent) of cyber attacks target small businesses. The threats are growing and changing as fast as online technology, and following are the types of cyber attacks criminals are plotting against your small business right now.

The Denial of Service (DoS) Attack

A DoS attack is a kind of internet piling on. These attackers send enough information and data all at once from multiple computers to overload your system so it shuts down. These are common and one of the best ways to prevent against this kind of malicious cyber traffic jam is using analytics to monitor unusual spikes in traffic flow. Regular security software updates are another routine way of preventing these types of issues.

The Inside Attack

Small businesses don’t always need to look very far for the threat of a cyber attack. Some
of the most crippling breaches occur when past employees decide to misuse the access to data and information you’ve left in place. When people quit or get fired, you generally take the keys to the front door back when they go. Make sure you revoke their access to any data after their termination too.

If you leave this cyber door open, a disgruntled ex-employee can even use what’s called Ransomware against you. That’s where they hijack your mission critical data and hold it until you pay a price to get it back.

The threats are growing and changing as fast as online technology.

Malware

That’s one word that should set of off alarms bells whether you’re running an eCommerce store or a brick and mortar shop with an online presence. Malware is the catchphrase for any of the malicious software that lurks in the weeds of cyberspace looking to gain access to your system to cause some kind of damage. The phrase covers a large swath of worms, viruses, Trojan Horses and other pests like Ransomware. Antivirus software creates a good moat around your business, and you should always be wary of opening emails from people you don’t know.

Watch for pop ups promising needed updates that are really masking rogue software. Updating your firewall is a good move too.

Password Attacks

Unfortunately, there are some very good reasons why internet security experts tell you to make sure your small business passwords don’t use common words and phrases or easy to remember terms like a variation on the name of your company.

Cyber criminals can unlock the door to your sensitive data using just one password as the key. It’s such a common scenario, the pundits have even divided these types of attacks into three subcategories:

The Brute Force Attack

Imagine an old school safe cracker here. Instead of a stethoscope to listen for the clicks telling them they’ve found the right combinations, these modern day criminals use a program to try different sets of common words. If a hacker has a list of employee names, they’ll get to work with easiest-to-guess passwords based on first and last names and pet names.

Changing passwords frequently can throw any hackers off your trail. Stay away from simple keyboard progressions like qwerty and away from slang terms and common misspellings. Once again comprehensive security software works wonders for your small business.

Cyber criminals can unlock the door to your sensitive data using just one password as the key.

The Dictionary Attack

Pretty much the same as the brute force version with a more narrowed focus. This attack gets it’s name from the fact that many people tend to choose passwords that are seven characters or fewer — the kind that can be found in the dictionary.
Where you login plays an important role. Unsecured WiFi connections are public and more open to being hacked.

**Key Logger Attack**

Imagine someone being able to use a program capable of tracking every keystroke you make? Hackers have access to programs capable of this, programs capable of putting your passwords and sign in IDs in their hands. If you’ve ever logged onto a computer or into a portal using a username and password, you could be vulnerable.

Fight back using multifactor authentication. Here, you’ll outfit everyone with a password and some other form of authentication that slows hackers down. Quite often an access code is used as an added form of protection.

Rob Starr
Staff Writer
@robertstarr

**TYPES OF CYBER ATTACKS**
Don’t regard a cyber attack as a potential risk for your small business? Think again. Cyber crime is on the rise and hackers are increasingly targeting small businesses.

The big question therefore is: are you prepared for a cyber attack? Small business credit provider Headway Capital, has compiled data to help you check yourself.

Here are some questions every small business owner must ask to ensure they are prepared for a cyber attack.

11 Cyber Security Questions Every Small Business Should Ask

Does Every Employee Have a Strong Password?

More than half of all data breaches caused by weak passwords and yet just 24 percent of small businesses have a strict password policy in place.
Are Your Employees Required to Change Their Passwords Regularly?

Despite having a password policy in place, 65 percent of businesses do not enforce it. It should be mandatory for your employees to change their passwords regularly to protect data.

When Possible, Do You Use Two-Factor Authentication?

Add an extra layer of data security by enforcing two-factor authentication wherever possible. For example, by adding SMS authentication.

Do Your Employees Use Their Personal Smartphones for Work Purposes?

Chances of malware attacks are greater when personal phones and devices are used in the office network. To prevent data theft, give your employees secure work phones with a passcode.

Are You Backing Up Your Files?

Cyber attacks can make your confidential files completely inaccessible. It is therefore a good idea to keep local backups as well as an offsite server.

Does Every Company Device Have Antivirus and Malware Software Installed?

Make sure the updated versions of antivirus and malware software are installed and check devices before use.

Have You Limited the Amount of Employees with Admin Access to Only Those Who Absolutely Need it?

Give access sparingly and only to those employees who really need it. Importantly, make sure those employees are well educated on security issues.

Are Your Employees Trained in Recognizing Phishing Emails?

Phishing accounts for 49 percent of all cyber attacks, and it can be tricky for an employee to identify it. It’s important to train employees to ensure they do not respond to suspicious emails.

Do Your Employees Know Never to Give Sensitive Information to Supervisors Via Email?

Sometimes hackers create an email address that looks genuine and is in the name of a colleague. Ask your team to double-check email requests for sensitive information.

Do You Encrypt Databases and Customer Information?

Without encrypting, your sensitive data is accessible to hackers. That’s why, you must ensure all your information is encrypted.

Are Your Websites Properly Protected?

Most attacks happen on WordPress websites. It’s therefore a good idea to install updates and stay updated on WordPress security best practices to avoid data loss.

Shubhomita Bose
Staff Writer
@ShubhomitaB
Exciting Travel Offers

Ignite Your Travels With Wholesale Travel Discounts

Save Up To 70% On Your Travel

Sign Up
Defeating Cyber Attacks on Your Business Will Require Humans and Automation

To defeat cyber crime, humans and robots are going to have to learn to work together. A new McAfee report released today sees a best case scenario where human “threat hunters” team with automation and machine learning technology to fight back against digital thieves.

The Need for Cybersecurity Automation

The report — Disrupting the Disruptors, Art or Science? — makes it clear humans acting without help can’t deal with the volume of data needed to thwart cyber attacks. It also stresses that one hand washes the other when it comes to the partnership between humans and technology in the fight against cyber attacks.

Humans on the Hunt with Sophisticated Tools

The new report classifies companies as mature and immature. The immature ones give their human cyber criminal hunters sophisticated tools and data and turn them loose in an ad hoc manner. But as these businesses mature, they come to rely on automation, analytics and other tools and refine their hunting techniques. The survey shows that once these processes
are fully intertwined, the companies that are the most mature are more than twice as likely to automate large parts of their cyber crime investigations.

Humans and robots are going to have to learn to work together.

Closed Investigations

The results are 70 percent of these investigations are closed in a week or less. This compares with a rate of less than 50 percent for companies that haven’t optimized this balance between humans and machines.

Mo Cashman, Enterprise Architect and Principal Engineer for McAfee makes an important point about not putting the cart before the horse in the company’s Threat Hunting Report Executive Summary.

The Right Technologies

“This research highlights an important point: mature organizations think in terms of building capabilities to achieve an outcome and then think of the right technologies and processes to get there. Less mature operations think about acquiring technologies and then the outcome,” Cashman writes.

The tools these firms use also vary with their maturity levels. For example, the organizations classified as the most mature are more than three times more likely to consider using various automation tools. These include user behavior analysis, endpoint detection and response as well as sandboxing. As the name suggests, sandboxing is about isolating suspicious programs or code so they can be tested separately without endangering your systems.

Successful teams fighting cyber security breaches use a tried and tested process.

Customizing and Optimizing

Customizing and optimizing also play key roles for the more successful organizations. Security Information and Event Management (SIEM) coupled with custom scripts are just two of the techniques used to automate processes. The human cybercrime fighters working in more mature firms spend 70 percent more time customizing techniques and tools.

Threat Intelligence

The report also underlines the correct use of threat intelligence as another secret sauce to getting the best results.

Human Decision Making

The processes comes down to combining human judgement and intuition with pattern recognition and speed of automation. The report also stresses that human decision making can make a big difference. It notes successful teams fighting cyber security breaches use a tried and tested process. The
Observe, Orient, Decide, and Act template was first documented by U.S. Air Force Colonel John Boyd.

The McAfee report surveyed 700 IT and security experts from firms with 1,000 to more than 5,000 employees worldwide.

After your business has lost data, it’s too late to think what you might have done.

Implications for Your Business?

Realistically, if you start your business from a laptop on your kitchen table or in the den, you may not have an IT team. But it’s probably a mistake to believe you’ll be too small to avoid the notice of cyber criminals.

And after your business has lost important client data, it’s too late to be thinking what you might have done. One thing the MacAfee survey highlights is the partnership between human judgement and automation.

Even in the early days, look for software and apps that can help you automate some of your security. You’ll need to pay attention and update your systems regularly when patches and security improvements become available. Combine human judgement and automation to keep your data safe even when you can’t afford an IT team.
The Verizon Data Breach Investigations Report for 2016 tells us 63 percent of small business hackers take advantage of weak passwords. What’s more, almost all (93 percent) took mere minutes to compromise systems. It all spells big trouble for America’s small business unless you focus on beefing up your passwords and adopting a policy. Follow these 20 password policy best practices to keep your company secure.

**Understand What Password Policy Is**

First you need to walk before you run. Understanding what a password policy is the first step in being able to build a strong one. These are a set of rules covering how you design the combinations of words, numbers and/or symbols that grant access to an otherwise restricted online area. Passwords can protect your website, software programs and small business networks. They keep them safe from unauthorized entry from ex-employees, curious intruders and of course hackers.

Follow These 20 Password Policy Best Practices to Keep Your Company Secure
Adopt the 8 + 4 Rule

This rule helps you to build passwords that are strong as steel. Use eight characters with one upper and one lower case, a special character like an asterisk and a number. The more random the better.

Keep Symbols/Numbers Separate

Here’s another hint for an effective password policy to foil hackers. Make sure the numbers and symbols are spread out through the password. Bunching them up makes the password easier to hack.

Don’t Make it Personal

Everyone involved in a small business needs to understand there’s a big difference between security and convenience when it comes to passwords. It needs to be clear using personal information like your first name and birth date is a recipe for disaster. If a hacker ever gets his hands on company HR data, this information will be the first set of combinations he tries.

Use Different Passwords for Different Accounts

Even if there are several computers in the same department, it’s a bad idea to cut a corner by using the same password for each. Use a different one for every device.

Avoid Dictionary Words

It might sound safe to go to the dictionary for a password, but hackers actually have programs that search through tens of thousands of these words. Dictionary attack programs have been around for years.

Keep the Character Limit Down

The average person can only remember 10 characters or less. Long passwords run the risk of being written down so they can be remembered.

Adopt Passphrases

Abbreviations are usually immune to dictionary attacks. So TSWCOT for The Sun will Come Out Tomorrow is a good choice for a secure password. Remember to add symbols and numbers.

Don’t Change Them Too Often

A good strong password will last for a year or more. Don’t encourage employees to change them any more frequently than that. Otherwise you can wind up with a password 1, password 2 situation. Hackers look for these patterns.

Don’t Write Anything Down

Granted, committing all of all your passwords to memory might get tricky. However, everyone under your small business roof needs to understand not to write anything down. A discarded Post-It can be all a would be hacker needs.
Discourage Sharing

No one should share passwords over any electronic media. If you can’t find a way of sharing a password without using cyberspace, make sure everyone knows to change it right away afterwards.

Add Other Barriers

When you’re putting together a password policy, make sure to look at the bigger picture. Well designed passwords put a good lock on the online front door of your company. More robust authentication like a fingerprint scanner make your small business safe like Fort Knox.

Encourage Weirdness

In the passwords and not your employees, that is. Still, they should understand the best passwords avoid pop culture and sports terms and anything that’s common. Random groupings of the 8+4 rule works but so do unique phrases.

Set a Lockout

We’ve all legitimately forgotten a password and need a few tries to get back in. However you should set a number that will lock the user out after a few unsuccessful attempts. Four failed logins works.

Stay Away from Acronyms

Don’t use these as a shortcut to identifying your department or who you are. It might be tempting for an accountant to use CPA. However, that opens a cyber security door wide enough for a hacker to walk right through.

Never Use Remember Password

Search engines and email programs mean well when they ask you this, but in the end it’s just another risk your small business doesn’t need to take.

Never Tell Anyone Your Password

A good policy will stress that no one should ever tell anyone else their password. The systems administrator needs to play gatekeeper here. If someone wants to know a password, they need to go to them.

Keep the Process Private

Finally, stress to everyone involved they need to hide the process from prying eyes. No one should be watching when you type in your password.

Adopt Stronger Policies for Sensitive Accounts

Administrators need to have more robust rules for setting passwords. The more data they have in their electronic baskets, the stronger the policy needs to be.

Rob Starr
Staff Writer
@robertstarr

Well designed passwords put a good lock on the online front door of your company.
Win with the Cloud

Generate new revenue streams with Cloud IP

Apply to secure $2000 Credit towards your Cloud IP Development

Apply Today
The 2016 State of SMB Cybersecurity Report from cybersecurity software company Keeper found hackers have breached half of the 28 million small businesses in the U.S. With small businesses becoming increasingly under cyber-security and data breach threats, it’s vital they have a comprehensive and solid data breach response plan in place.

10 Things Your Small Business Data Breach Response Plan Must Have

What You Need in a Data Breach Response Plan

If you’re a small business looking to make the wise move of implementing a data breach response plan into the culture of your business, take a look at the following ten things that every small business data breach response plan should include.

Determine How Vulnerable You Are to an Attack

Which industry do you operate in? Some industries are naturally more vulnerable to cyber-attacks than others. According to the 2016 IBM X-Force Cyber Security Intelligence Index, healthcare comes out on top of the most cyber-attacked industries.
Determining how vulnerable your business is to falling victim of a data breach should be the first thing you research when devising a response plan, as this will give you a clearer picture of how much time, money and effort should be put into a cyber-attack response strategy.

Some industries are naturally more vulnerable to cyber-attacks than others.

**Identify Data That Constitutes a Data Breach**

Every data breach response plan needs to define the type of data that would constitute a data breach. Generally speaking, data that contains customer and employee information, such as credit card numbers and social security numbers, would create serious issues for a business if stolen or compromised.

State and International laws require victims to be informed if such data has been compromised. It is therefore vital that the security of such data is prioritized in a data breach response plan.

**Classify Data Assets**

Once you have identified what your business’s primary data assets are, classify them in order of importance. Make the classification system simple and easy to follow, compromising of High, Medium and Low assets.

This way, if a breach occurs, you’ll know which assets need to be given priority over others.

**Empower the Response Team**

When devising your response plan, spend time empowering a response team. In order to save your business money by having to bring in outside help, align the response plan with existing business continuity plans. Consequently, the response team will be able to make effective and timely decisions in the wake of a data breach.

**Who Is Responsible for What During a Data Breach?**

State and international laws require victims to be informed if such data has been compromised.

When working on the responsibilities of the response team, map out precisely who takes on which roles if a breach of data should rear its head. This is a cost-effective and easy-to-implement way to help limit the amount of damage and control processes in the wake of a security breach.

**Create a Communication Plan of Attack**

Your data breach response plan should include a communications strategy, which outlines how the likes of employees, customers or even...
the public would be notified and communicated with in the event of a cyber-attack.

If you’re a small business on a tight budget, ensure the plan includes a cost-effective communications’ strategy, such as using social media or email notifications to inform stakeholders if a security issue had arisen.

Align the response plan with existing business continuity plans.

When You Might Need to Bring in External Help

Small businesses typically have small teams, which lack in IT, security and other specialized professionals. Part of your plan should include at what point when a data attack occurs will external support, such as IT and security practices, be brought in.

Get the Right Legal Support

A breach of valuable data can create a legal minefield and for small businesses, the costs associated with rectifying such a legal minefield can be eternally crippling.

It is therefore imperative to have a legal support team in place to deal with the legalities of the breach to help limit the damages should a breach of vital data occur.

Make Data Breach Insurance Requirements Part of Your Response Plan

If a small business has its data compromised without any data breach insurance in place, the financial and reputational damage the cyber-attack can create, can be enough to end the business.

Cyber breach insurance offers protection and support to businesses that become victim to a data breach.

When devising your data breach plan, spend time determining whether to take the precaution of taking out data breach insurance. If you do decide to pay for such insurance, be sure to include the details of the insurer in your plan, such as the phone number and policy number, so you can contact them with ease, should an attack take place.

Practice Makes Perfect!

Once you have a solid data breach response plan in place, don’t just hide it away and forget about it until you need to rely on it when an attack happens. Practice the plan and its different steps with your team, regularly.

Running through the plan won’t take up too much time or require a large investment of money. What it will however mean, if a breach does occur, your small business is ready for it!
When you think of cyber attacks, you may imagine complex campaigns against major corporations and governments. The reality, however, is far more common and serious – especially for small businesses.

**Phishing Attacks Pose a Huge Threat to Your Small Business**

Hackers often trick well-meaning employees into giving access to their business systems by getting them to unwittingly click on a link in an email. This method of cyber attack is known as phishing — and it’s on the rise.

But what’s perhaps even more worrying is that most employees may not even be able to identify phishing. That’s according to data published by Texas-based eLearning company, Inspired eLearning.

Statistics reveal 97 percent of people cannot identify a sophisticated phishing email — putting confidential business data at risk.

Consequently, businesses end up losing a lot of money. The study suggests phishing scams cost businesses about $500 million a year. For a small business, the impact is understandably much bigger.
Hackers often trick well-meaning employees into giving access to their business systems.

**Protect Your Business Against Phishing**

The Anti-Phishing Working Group (APWG) found phishing attacks have been dramatically rising since 2004 with a 65 percent increase from 2015 to 2016.

The ever-increasing threat of phishing scams makes it even more important for small businesses to revisit their security features.

The next step is to boost the security features at your business to prevent data breaches. Investing in a robust data security infrastructure will help you monitor for suspicious activity on the network and protect your business.

**Train Employees to Identify a Phishing Attack**

But the most crucial aspect to be considered is employee education, as 91 percent of hacking attacks start with phishing emails. It pays for businesses to train employees to identify a phishing attack that arrives via email. Emails asking for sensitive data such as passwords and personal information are most likely phishing emails that employees must recognize.

---

*Shubhomita Bose*

Staff Writer  
[@ShubhomitaB](https://twitter.com/ShubhomitaB)
Cyber security breaches cost businesses billions of dollars each year. Breaches in 2016 reached a record peak. Data from the Identity Theft Resource Center reveals in 2016, U.S. businesses and government agencies suffered a record 1,093 data breaches, a 40 percent increase from the previous year.

According to Deloitte, the current market valuation of cyber incidents is grossly underestimated.

As Emily Mossburg, a principal with Deloitte Touche Tohmatsu LLP and resilient practice leader for Deloitte Advisory cyber risk services, notes, “An accurate picture of cyber attack impact has been lacking, and therefore companies are not developing the risk posture that they need.”

The impact a cyber-attack can have on businesses can be devastating. Given the rise in frequency and intensity of these breaches and the damage they cause, taking out data breach insurance could be a wise move for businesses.
What is Data Breach Insurance?

Data breach insurance is designed to protect and support a business if it becomes the victim of a cyber-attack. This specific type of insurance provides comprehensive cover in the event of a claim related to a malicious cyber-attack or breach of data.

Data breach insurance offers protection if a hacker attempts to hold a business to ransom. The insurance can cover the ransom you are forced to pay the hacker, as well as helping you manage the whole stressful situation.

Comprehensive data breach insurance will also offer practical support in the event of a cyber-attack on your business. Such support includes providing a business with legal advice, forensic investigations, notifications to clients, customers and regulators and support to affected customers, such as credit card monitoring.

A cyber attack that targets a business’s systems can even prevent a company from earning revenue. This disruption caused by cyber hacks and security breaches can lead to businesses experiencing a significant loss of income. Data breach insurance can provide compensation for such loss of income, including where the hack has created damage to a business’s reputation.

Virtually any business that relies upon and stores data is at risk of being hacked.

What Small Businesses Might Need Data Breach Insurance?

Does your business create and store sensitive data? If data is one of the most important assets of your business, you should consider getting protection from potential hacks and data breaches.

If your business holds customers’ personal data it may be particularly vulnerable to data breaches by hackers who seek to steal personal information and use it fraudulently. Data such as bank account information, customer records, social security numbers and credit card numbers, make appealing targets for cyber criminals. Breaches of such valuable information could then lead to liability claims made against your company, putting your business’s reputation in serious jeopardy.

If your business has a network on which employees save data and a virus gets into the network, your company could be at risk of a data breach.

Naturally, some industries are more data-reliant than others. Some of the most heavily targeted businesses by cyber criminals include financial services, healthcare providers, manufacturers and retailers.

Business owners operating in these categories need to take measures to protect their companies, employees, customers and data from such threats. That said, few businesses are entirely immune to the threat of cyber crime. Increasingly sophisticated cyber criminals leave no stone unturned in their quest to seek out data that doesn’t belong to them.

You may be a solopreneur operating a one-person marketing business from home. Or you may operate a mobile hairdressing business and store personal information of customers on a computer. Virtually any business that
Natalie Cooper, editor of BankingSense, reiterates the importance of cyber liability insurance for small businesses, stating, “For small businesses, nothing is more important than protecting their livelihood. Cyber liability insurance is another tool they can use to prevent financial disaster in the event of a malicious attack.”

The impact a cyber-attack can have on businesses can be devastating. Some of the best data breach insurance policies cover the associated costs of the breach, including forensics, customer alerts, legal fees, crisis management and consumer identity monitoring.

Regardless of the size of business you operate and the industry you work in, if you store sensitive data, investing in data breach insurance would be an invaluable move in protecting your data, and safeguarding your business from attack.
If your small business hasn’t been “hacked,” it can be difficult to quantify the potential impact of cyber crime.

True the impact of a cyber crime committed against your small business can range from simply annoying to potentially crippling. But in the end, the question remains whether a way exists to measure that impact in dollars and cents?

Cost of a Data Breach

Well, new data from cyber security software provider Symantec (NASDAQ:SYMC) and eCommerce platform BigCommerce reveals the true cost of a hack on an eCommerce retailer. According to that data, the cost of a data breach to an eCommerce retailer is now $172 per record.

And the cost to eCommerce retailers continues to increase as does the likelihood of an attack. The same data shows that the cost of a hack has gone up 29 percent since 2013. Today, the
average cost of a single attack stands at a staggering $4 million.

The impact of a cyber crime committed against your small business can range from simply annoying to potentially crippling.

Three Pronged Attack

Hackers are predominately using three types of attacks on eCommerce retailers.

A denial of service attack (often referred to as a DDoS attack) is the most common attack. BigCommerce and Symantec data shows that 45 percent of the attacks on eCommerce companies are DDoS attacks.

Attacks on a point-of-sale solution (32 percent) or a web app (13 percent) were the two other most common against eCommerce retailers.

A Lesson Churned

Probably the most negative impact of a security breach on an eCommerce retailer is the loss of business. Many existing customers who have had their data compromised and those who might have been your customers may cease doing business with you.

And this is where the cost of a cyber attack begins to mount.

Data collected by BigCommerce and Symantec shows U.S. eCommerce retailers may face their greatest challenge winning back customers following a data breach.

In fact, the data suggests such an attack may increase a company’s churn by 2.9 percent.

The average cost of a single attack stands at a staggering $4 million.

Get Ahead of It (If Possible)

Of course the best way to minimize the cost of a data breach is to be prepared when it comes.

For example, data from Symantec and BigCommerce suggests eCommerce businesses can save up to $16 per hacked record simply by having an incident response team in place to deal with an attack when it happens.
Is Your Office Equipment Cyber Safe? New Ratings Standard Rates IoT Products

More of the things we use in business and life are now connected. This makes them much smarter and more efficient, but also susceptible to security vulnerabilities. For small businesses and solopreneurs, keeping track of which equipment is safe or vulnerable can be a task in itself, which is why the Digital Standard launched by Consumer Reports may help in this effort.

The connectivity of office equipment is pretty much part of the landscape now, but as the Internet of Things (IoT) continues to evolve, the level of connectivity of all devices is becoming more relevant. And because office equipment and other device manufacturers don’t all necessarily take the same steps to address the security threats, the problem is likely to get worse before it gets better.

The way Consumer Reports has decided to tackle the problem is with the Digital Standard. In collaboration with industry players, it seeks to put data security and the privacy needs of technology users — including small businesses — first.
It seeks to put data security and the privacy needs of technology users—including small businesses—first.

Introducing the Consumer Reports Digital Standard

Collaborating on the new Digital Standard are Disconnect, creators of technology that helps block data collection and tracking, Ranking Digital Rights, an organization that grades companies on their commitment to user privacy, the Cyber Independent Testing Laboratory which advises users about software safety and Aspiration, a funding service focused on ethical investing.

In a release announcing its launch, Consumer Reports President and CEO Marta L. Tellado explains, “While the pace of new technologies is exciting and brings greater convenience to our lives, it also carries with it new threats to our security and personal privacy.”

This threat was highlighted in 2014 when Proofpoint reported routers, smart TVs, and at least one smart refrigerator were used to launch a cyber attack. For small businesses and solopreneurs who may use smart devices like printers, scanners, 3D printers, cameras and more in their day to day operations the concern becomes even more relevant.

In its effort to create a digital privacy and security standard, Consumer Report creates a new bar for companies that produce smart appliances, mobile apps and software. The standard will also identify and address the kinds of risks users including small businesses face with digitally connected products when it comes to data security and privacy.

The standard also extends to protecting personal information products, apps and services after they have been purchased, with the goal of putting in place protection measures that are more stringent in the marketplace.

Michael Guta
Staff Writer
@mmguta
You’ve no doubt heard about some of the cyber attacks that have impacted large businesses and even governments in recent years. But small and medium sized businesses can fall victim to similar types of attacks as well.

Strongarm is a small business that aims to help those small and medium sized businesses avoid cybersecurity issues.

**What the Business Does**

Provides security to small and medium sized businesses.

Co-founder and Chief Technology Officer Todd O’Boyle told Small Business Trends, “Strongarm provides cloud-based, automated, and simple-to-use security that focuses on stopping attacks from damaging small and mid-sized businesses and speeding the process of cleaning up cybersecurity infections.”

**Business Niche**

Providing personal service.
O’Boyle says, “We’re known for “team and touch.” Our team will talk to you every time we protect you from a cyberattack, not just when your license is up for renewal. We get to know our customers personally. Strongarm was built from the ground up to be simple and easy to use while most security solutions are more complicated with way too many features and complexity than is needed.”

Strongarm was built from the ground up to be simple and easy to use while most security solutions are more complicated.

How the Business Got Started

In a government lab.

O’Boyle explains, “Strongarm was built in a government lab at The MITRE Corporation. Our Vice President of Engineering Stephen DiCato and I were principal investigators there. In 2013, we met Allied Minds and they were interested in commercializing technology from government labs. They supplied us with seed money and we joined as the first two employees. We’ve been at it for two and a half years now.”

Biggest Win

Getting their first customer.

O’Boyle says, “Our biggest win was the first time anyone paid us for our product. We found the customer through an old MITRE Corporation contact that worked as a security analyst. The customer is a global financial solutions company with 1,500 employees and has a somewhat mature information security team of three to five people. They weren’t finding any sophisticated security solutions in their price range until they found us. It wasn’t a lot of money at the time, but they’re still a customer and are now our biggest customer. They’re one of the customers that drives our product features and they’re early adopters of everything that we launch.”

Biggest Risk

Targeting small businesses.

O’Boyle explains, “The biggest risk we have is our customer focus – SMBs. Large customers bring large revenues and float you to more fundraising more quickly. With our SMB focus, we need to better understand their businesses to shorten the sales cycle and we also need to scale to a larger volume of SMB customers. Achieving this scaling is something we work on every day.”

Lesson Learned

Don’t always take the easy road.

O’Boyle says, “When you’re starting a business, there are a million different ways you can take it. Many times entrepreneurs take the seemingly “easy road” by partnering with big companies or with original equipment manufacturers (OEMs) that sell their solutions. We did this as well. In hindsight, I would have not spent the first year and a half chasing big deals that wound up going
nowhere. If I could go back, I would have gotten out and hustled more to talk with potential SMB customers about our product.”

**How They’d Spend an Extra $100,000**

**Customer outreach.**

O’Boyle says, “We have an awesome product and to achieve the volume growth for the business, I would spend the extra $100K doing more outreach to SMBs where we can get out and talk to more SMBs face to face.”

**Team Drink**

“The Bobby.”

O’Boyle explains, “The official company drink is “The Bobby”, named after our first salesperson, Bobby Preston. It consists of a late afternoon espresso plus a glass of plain Polar seltzer. In fact, all of us drink a ton of Polar seltzer – more than we were designed to consume with only one bathroom in the office! Although we like almost all the regular flavors, as opposed to the seasonal flavors, cranberry lime is the clear winner.”

**Favorite Quote**

“Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away.” -- Antoine de Saint Exupery

---

**SPOTLIGHT**

**Build New Revenue Streams with Cloud Technologies**

Offer ends by April 30th, 2018

APPLY NOW
One day I was perusing an article about some new tech product and someone in it said something to the effect of “is it a perfect idea? No.”

Then later, they kept going. “Did it turn out like we thought it might? No.”

And it struck me that this was something you could keep going with for a while in a cartoon. The tough part was finding multiple ways to say “no” that sounded conversational.

Did it turn out well?
Yes.

Am I happy with it?
You know it.

Should I keep this up?
Probably not.
Would you like your message to appear in Small Business TRENDS Magazine?

Get in early - contact us: advertise@smallbiztrends.com