
The MSP's Complete Guide to Cyber Security
Barracuda MSP

CONTENTS

INTRODUCTION 3

COMMON CYBERSECURITY MISTAKES YOUR SMB CUSTOMERS ARE MAKING 5

5 TIPS FOR APPROACHING CUSTOMERS ABOUT CLOUD SECURITY 7

WHAT YOU NEED TO TEACH CUSTOMERS ABOUT RANSOMWARE 10

HOW TO DEVELOP A SECURITY POLICY FOR AN SMB CUSTOMER 13

CONCLUSION 16

ABOUT BARRACUDA MSP 17

Introduction

With massive data breaches making headlines on a regular basis, it's hard to ignore the fact that data security is becoming increasingly important. Unfortunately, there are still far too many SMBs that don't understand just how serious the threat is—and that can be dangerous.

Growing threat to SMBs

Recent research demonstrates that the growing cybersecurity threat isn't a trend affecting only big, national companies. It's just as serious—if not more serious—for small businesses to be prepared because data breaches and cyber attacks are very real possibilities for them. According to Ponemon Institue's 2017 State of Cybersecurity, cyber attacks affected 61 percent of SMBs in the past 12 months[1], and the number of data breaches reported each year continues to climb. If that's not alarming enough, these companies on average lost more than 9,350 individual records as the result of a breach[1].

Educate your customers

Cybercriminals will do anything to get their hands on sensitive data. According to Ponemon's study 54 percent of SMBs admitted they had a breach involving sensitive information about customers, target customers, or employees[1]. Educated employees are still the best line of defense when it comes to cybersecurity, which is why it's important to start the conversation now.

To help you prepare for these conversations, we've gathered our best cybersecurity advice on the following topics:

- Common cybersecurity mistakes your customers are making
- Tips for approaching customers about cloud security
- What you need to teach customers about ransomware
- How to develop a security policy for an SMB customer

54%

say that negligent employees were the root cause of a data loss.[1]

Start the conversation: Don't wait until something goes wrong. Be proactivce. Customers might not think they need a cyber secruity solution, but talking to them about the dangers they face without one might change their mind.

To learn what new threats are emerging, visit Barracuda's Security Threat Index.

Common cybersecurity mistakes your SMB customers are making today

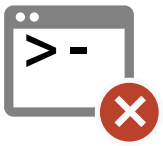
Bad habits are hard to break, and that's especially true when it comes to small businesses and cyber security. After all, it's easy for SMBs to ignore cyber security because they think "that will never happen to me." But, letting things slide can end up creating real security concerns. As a managed service provider, you need to communicate with your customers and educate them about what to do and what not to do to avoid unnecessary risk.

Here are a few common errors you'll need to watch out for with your SMB customers:

1. The Post-It full of passwords

The next time you're at a customer's office, take a walk around. Most likely, you'll find at least a few desks with Post-It notes full of passwords stuck to the bottom of a computer monitor. Yes, it's convenient, but it also provides easy access to sensitive information to people who shouldn't have it—like disgruntled employees or a thief during a break-in.

The Fix: Take the opportunity to explain to your customer why this is a bad idea, and give them some ideas on how manage passwords safely.



2. Out-dated operating systems

Technology is an important part of every small business, but it's often not a priority. That's how things like updating operating systems fall through the cracks or get ignored until they become a serious security threat. For example, do any of your customers still have systems running on Windows XP or Windows Server 2003? If they're running a more recent operating system, are they keeping it up to date? If you don't know, find out.

The Fix: If you do have clients running outdated operating systems, it's a good opportunity to help them transition to something more secure. Even better, you can use it as a chance to initiate a managed service contract to take care of updates and patches going forward.

3. Security software that never gets updated

Some small business owners think they're secure because they invested in a firewall or installed antivirus software on their machines. But odds are they didn't take the next step and pay for subscriptions or updates to go with it, which means they aren't nearly as secure as they think.

The Fix: When you talk to customers about cyber security and they say they have programs in place already, ask when they updated that software. Most likely, they won't have an answer. That means there's another good opportunity to establish an ongoing managed service handling security updates for that client, and that translates into more recurring revenue for you as an MSP.

4. Old employees still have access

Lax password policies and passwords that don't expire create another security concern for SMBs. If your customers don't set passwords to expire regularly, there's a good chance a number of former employees still have access to their system. That doesn't necessarily mean any of them will do something malicious, but why take the risk?

The Fix: Help your customers set up a solid password policy, and explain why it's important to have passwords that expire regularly. Yes, their employees might think it's a hassle at first, but the improved security will be worth it. While you're at it, help your customers teach their employees the best practices for choosing a strong password that's easy to remember but hard to guess.

Use these common cyber security mistakes as learning opportunities for your customers. Teach them why cyber security matters and what they can do to help make their businesses safer. And stress the value you can bring as an MSP by helping them address their security concerns.

5 Tips for Approaching Customers about Cloud Security

For managed service providers, network security can feel like something you have to shove down customers' throats. Why? Because most small business owners don't fully understand the growing need for security or what the return on investment will be.

When selling cyber security to their SMB customers, most MSPs run into challenges due to budget restraints and a lack of knowledge. The typical small business doesn't have a huge technology budget to properly secure their network, so they end up compromising on security to get the performance they need within the budget constraints they have set aside to work with.

To help bridge the gap and equip yourself to better discuss the topic of cyber security with your customers, the following infographic, "5 Tips for Approaching Customers about Cloud Security," provides a list of best practices to follow.

1 Explain It's Not If You Need Security, But What Type of Security You Need

Start the cyber security conversation with the level of security they need, and present options based on their business type.

*43% *of all attacks happen to small businesses*

*Microsoft, "2017 Small Business Insights Survey"

2 Talk About the Dangers of Having Insufficient Security

Without a comprehensive security solution, businesses can not only lose important data-but permanently close their doors.

*50% *of small businesses are not concerned about a data breach*

*Microsoft, "2017 Small Business Insights Survey"

continued

3 Educate That the Cloud Is More Secure Than On-premise

A "cloud" of fear surrounds storing data in the cloud, but in fact, on-premise security solutions are more susceptible to attacks and threats.

* Storing data on-premise

=

Storing money under your mattress

Storing data in the cloud

=

Storing money in a well-protected bank

4 Relate Cyber Security to Physical Security

People buy physical security such as alarms and locks without batting an eye. Customers should think of cyber security the same way – as an investment.

*25% *of small businesses are doing nothing to protect themselves*

*Microsoft, "2017 Small Business Insights Survey"

5 Inform How Cloud-based Security Helps With Industry Compliance

Cloud-based security solutions with proper encryption protect data from intrusion and the latest threats, storing customer information in compliance with various industry standards.

**Cloud-based security solutions meet HIPAA, PCI, SOX and FINRA standards*

*Cloud-based security solutions meet HIPAA, PCI, SOX and FINRA standards

40

Every 40 seconds a business falls victim to a ransomware attack. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019.[3]

A 2017 report finds that the world will need to cyber protect 300 billion passwords globally by 2020.

300 Billion passwords[3]

What you need to teach customers to keep them safe from ransomware

Ransomware is considered a fact of life in today's cybersecurity landscape. For MSPs, it's a known threat, but that doesn't mean SMBs are protecting themselves from a potential attack or even know it's a possibility. Often, users recognize a ransomware threat after it's too late. In February 2018, according to Osterman Research and Barracuda Networks, there was one phishing attempt in every 3,331 emails and one piece of malware for every 645 emails.[4]

And falling for one of these emails can be costly. According to the Ponemon Institue, the average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053 in the past 12 months, and the average cost due to disruption of normal operations increased from $955,429 to $1,207,965.[1]

MSPs need to help protect their customers from the growing threat of ransomware, particularly CryptoWall and Teslacrypt, two of the most prevalent types of ransomware. Start by educating your customers about the threat of ransomware and sharing these important tips.

1. Put technical safeguards in place

As a best practice, have an intrusion-prevention system and security software running on your customers' computers. This should include antivirus software, firewalls, and spam filters. Then, make sure all security patches are up to date, and deploy new patches on a regular basis. Schedule a recurring meeting on-site so you can check to see if all these safeguards are working properly.

It's also critical to have a backup solution in place and frequently test the backups running on your customers' systems to make sure they're working properly. If a customer is hit with ransomware, you'll need to restore their operations as quickly as possible, and having a recent backup to recover from will save you both time and money.

2. Train employees

Even with technical safeguards in place, it's employees who ultimately risk exposing a business to ransomware. User error, such as clicking on an infected online advertisement, pop-up window, or attachment in a spam email, is often to blame for inviting ransomware into a computer. So, users are the most important line of defense.

Talk with your customers about ransomware, educating them on what it is and how they can defend themselves and their businesses. Try getting all the employees together for a training session and bring lunch to make it a Lunch and Learn event. If you're unable to meet in person, you can create an online training program with videos that walk them through each lesson.

Encourage customers to require all new employees to complete the training and offer it on an ongoing basis to avoid information being missed. If you don't have the resources to put this type of training together, you can always compile pertinent information in articles, guides, and quizzes and send them along in an email to the company.

3. Provide examples to end users

The most effective way to educate your customers on ransomware is to show them examples of what it looks like so they'll know the warning signs and be able to identify a suspicious message or attachment before they click on anything. For example, you can share Barracuda MSP's Ultimate Phishing Quiz, which includes examples of infected and legitimate emails and provides explanation of how to tell the difference.

Once ransomware has infected a computer, a message is displayed on the screen letting the user know their machine has been compromised. Examples of these messages can be found here. It's helpful to share this type of information with your customers as well so that, even if it's too late, they'll know to alert you and ask for help.

How to develop a security policy for an SMB customer

Many successful MSPs have developed formal, documented IT security policies to govern operations both in their offices and in the field. Equally important, they conduct reviews of these policies every few years, and revise them as necessary to adjust to changes in their environments and business practices. Naturally, their customers appreciate their expertise and ability to devise security policies to meet their business' particular needs.

To leverage the value-add in offering these types of services, follow these best practices for developing a security policy for an SMB customer.

1. Identify roles and responsibilities

First and foremost, find out who currently has access to critical data, infrastructure, and applications. Note your findings and then assess whether or not each person needs the access they've been granted. To do this, you need to interview key stakeholders to fully understand employees' roles relative to this data.

Once you have a better idea of individuals' roles in the organization, you can begin to limit or reinstate permission to access sensitive information and assets. For example, system administrators should have access to things that contractors should not. Part of your mission is to ensure that there will be no uncertainty about who has access to what.

2. Define data retention parameters

You'll also need to help the SMB implement a document retention policy. These types of policies are especially important in certain regulated industries that require specific retention parameters. Defining a data retention policy is critical because there's an increased risk of data being stolen or compromised when it's kept beyond those defined dates.

3. Verify robust encryption technology is being utilized

Setting standards for encoding your customer's information is another important part of a security policy. Implement military-grade 256-AES (Advanced Encryption Standard) encryption technology to secure customers' data stored in the cloud, and use SSL (Secure Sockets Layer) encryption technology for their data in transit. To make your security policy even stronger, look for a data protection solution that uses private key encryption (PKE) technology.

4. Adhere to compliance regulations

When developing a security policy for a customer, be sure to meet to their industry's compliance regulations. Certain industries are more regulated than others, but you should always inform customers of any pertinent regulations and make sure their security policy addresses all issues necessary to help them stay compliant. HIPAA, for example, requires all covered entities to encrypt all their storage technologies for data at rest. As an IT service provider, you'll need to determine what customers are liable for and make sure they comply with all requirements.

To learn how to secure your SMBs' inboxes,
watch the free, on-demand webinar
"Strategies for Stopping Email-Borne Threats"

Conclusion

With cybercrime becoming an increasingly serious threat, it's not a question of if businesses need security; it's a question of what level of security they need. As an MSP, you should keep this in mind as you begin reaching out to your customers about data security. To get the conversation started, try offering a health check where you inspect their systems to uncover any security vulnerabilities.

It's important to start educating your small business customers as soon as possible, though, because new cyber threats emerge every day. Be proactive and start talking about cybersecurity with your customers now instead of waiting until after they experience a data breach or malware infection. Don't wait until it's too late.

SOURCES

1. "2017 State of Cybersecurity in Small & Medium-Sized Businesses," Ponemon, Sept. 2017.
2. "Small Business Insights," Microsoft, Oct 15, 2017.
3. "2017 Cybercrime Report," Cybersecurity Ventures, 2017.
4. "Best Practices for Protecting Against Phishing, Randomware, and Email Fraud," Osterman Research on behald of Barracuda Networks, April, 2018.
5. "Navigating a Cloudy Sky," McAfee, April, 2018.

About Barracuda MSP:

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP platform. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.