SECURITY SPOTLIGHT

Small Business IT Security Practical Guide

How to make sure your business has comprehensive IT security protection

KASPERSKY lab

$86,500

Average total impact of a data breach for SMBs[1]

Cybersecurity probably sounds like something that large enterprises need to worry about. What could cybercriminals possibly want with a small- or medium-sized business (SMB)? The answer: An awful lot.

If you're a small business who acts as a vendor to a larger organization, your company's security vulnerabilities are a cybercriminal's opportunities. Do you send invoices to a large company? Do your employees send emails to them? Do you have confidential information in your database? Chances are, you have all of the above, which means that cybersecurity should be a top concern to protect your company's data, your employees' privacy and your client relationships.

Many smaller companies don't understand the enormous costs they could incur from a data breach. As noted above, just one data breach costs an SMB an average of $86,500. Is that in your budget? Is it in your budget in case it happens multiple times? And if it is a targeted attack, the average costs go up to $143,000.[2]

Our recent survey shows that **86% of small businesses worry about data loss**, specifically as a result of employees physically losing devices. They are right to be concerned. If a data breach goes undetected for longer than a week at an SMBs, an average of 70,000 sensitive customer or employee records are compromised.[3] And when it comes to Bring Your Own Device (BYOD), 54% of businesses have had data exposed because employees have lost devices. In fact, **employee carelessness contributed directly to 48% of cybersecurity incidents, even more than theft of devices.**

Clearly, cybersecurity should be top of mind if you are an SMB that has large enterprises as customers, maintains sensitive information in your database, or have employees that have access to sensitive information. In other words, it is something that should concern every business and no size business is immune.

Now that you know how important it is, what can you do about it?

1, 2, 3. *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Your security checklist

There are specific steps you can take to protect your company, and you don't need a degree in Information Technology or a background in cybersecurity to implement them.

☑ Multi-layered security solution

No IT department is an island. Having the right technology to back you up will ensure that your company is protected from all threats, including those that result from human error.

Having a robust, multi-layered security solution that predicts, detects, prevents and responds to threats is essential for any small business.

☑ Employee education

With 48% of cybersecurity incidents attributed directly to employee carelessness, you cannot afford to ignore employee education about cybersecurity. In fact, your employees are your first line of defense, but they often don't realize that they have a role to play. When they refrain from opening suspicious attachments or when they know how to alert the IT department when something does happen, your whole company is much safer.

In many companies, IT policies are written in such a way that they cannot be affectively absorbed by employees. Many companies give employees multi-page documents that everyone signs but few read or understand. Design employee education programs that are both fun and informative. Lunch and learns, games and prizes are a great way to engage people in this very important topic.

What is phishing?

Phishing is the ultimate social engineering attack that involves sending out emails or texts disguised as legitimate sources. They may look like they are from a trusted vendor or a law enforcement authority, but secretly, they contain malware. These messages are specifically designed to trick the victim into opening the email through the tactics of fear and intimidation. Once a person opens it, the malicious software downloads onto their computer, and the cybercriminal is in your system.

See our eBook *The Dangers of Phishing* for more information on this dangerous tactic.

Passwords

Employees also need to make sure they're using strong, unique passwords that mix symbols, numerals and letters of both cases. Everyday words can be cracked by programs that simply scan through dictionaries until they find the right one. And even if it's strong, if a compromised password is used for multiple purposes, it could lead to an even bigger breach.

Patches and updates

Cybercriminals tend to exploit vulnerabilities in software to compromise systems. For this reason, it is essential to set aside a time to run patches and updates that are regularly issued by software companies.

With Kaspersky Lab's automated Vulnerability Assessment and Patch Management tools, you can rest assured that your system will be scanned and that patches will be distributed regularly in order to keep your system updated.

Make sure you don't make any of these classic password errors:

1. Using easy-to-remember but easy-to-guess options such as "password" or "123456"
2. Using your email address, name or other easily obtainable piece of data as a password
3. Setting password reminder questions a hacker could answer with just a little research – your mother's maiden name for example
4. Making only slight, obvious modifications to regular words, such as placing a '1' at the end
5. Using common phrases. Even small sentences such as "iloveyou" are easily cracked

54% of businesses have had data exposed because employees have lost devices.[4]

Bring your own device (BYOD)

More and more small- and medium-sized companies are adopting BYOD policies as a convenience for employees and a cost saving measure. But many problems can arise if it is not managed properly. Ultimately, successful BYOD implementation is dependent on employees following the rules, especially when it comes to loss of devices that may compromise sensitive data.

With 40% of businesses around the world reporting that employees hide security incidents when they happen,[4] make sure that your people feel comfortable to report any incident that occurs with their devices, especially loss or theft.

Encryption

More and more small- and medium-sized companies are adopting BYOD policies as a convenience for employees and a cost saving measure. But many problems can arise if it is not managed properly. Ultimately, successful BYOD implementation is dependent on employees following the rules, especially when it comes to loss of devices that may compromise sensitive data.

4. *The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within*

Understanding the risks

Some cybersecurity stories are legendary. Take note of these cautionary tales, and make sure that your company doesn't have an entry into this notorious hall of fame.

A very expensive cup of coffee

Having waved goodbye to the last client of the day, Thomas locks up and leaves work. There's a café just across from the office where he is due to meet a friend. Remembering that payment to one of his suppliers is due tomorrow, he decides to take care of it before he forgets.

He uses his laptop to connect to the café's WiFi network, logs into his bank's website and makes the transfer. Pleased it didn't slip his mind, he sits back and enjoys his coffee.

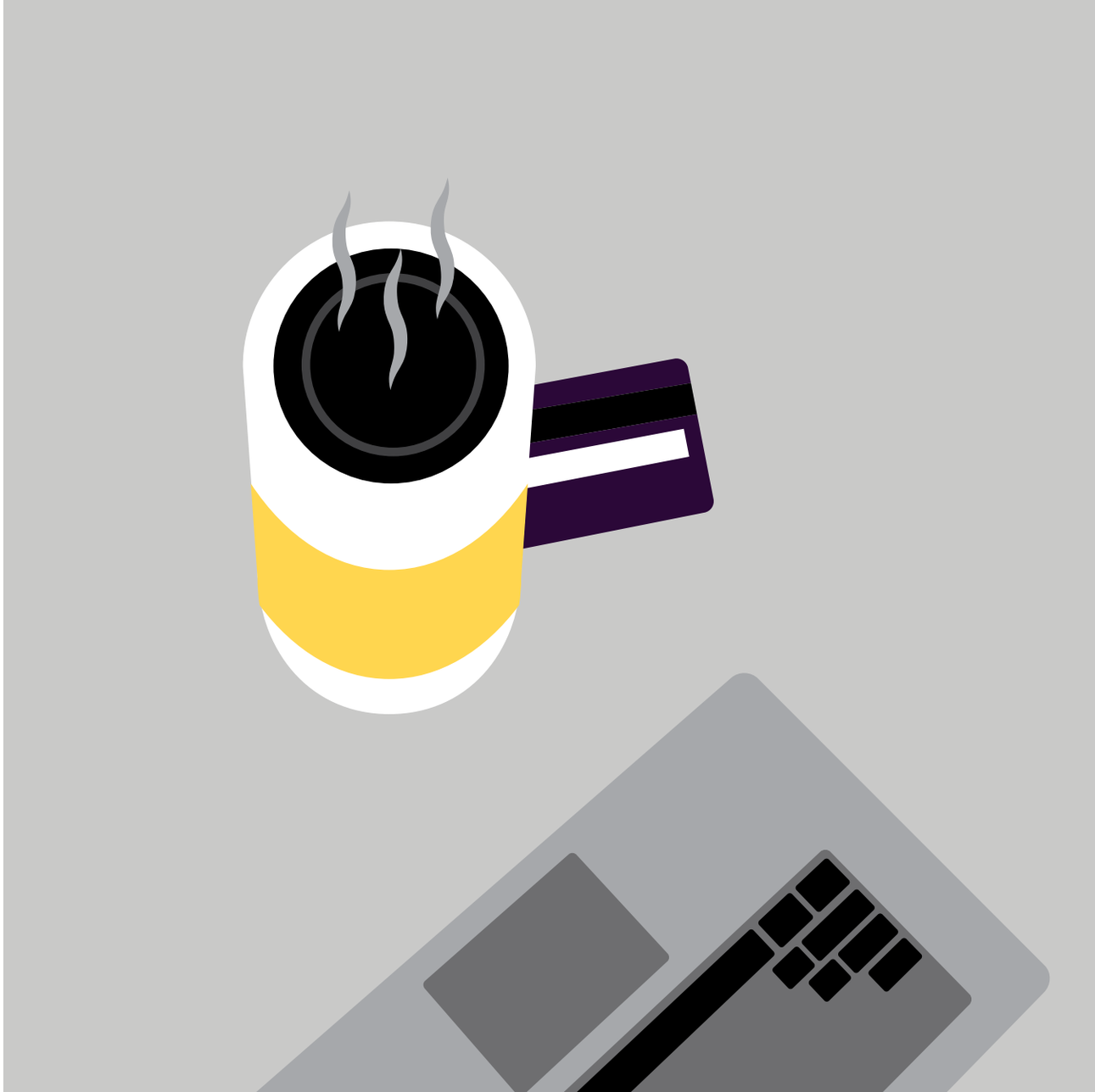
When he next checks the account, it's empty. While he's left trying to figure out why, his staff are waiting for their pay.

How did it happen?

Unfortunately, he didn't have any form of anti-malware installed and had picked up a malicious keylogging program. Those who launched the program received a record of all the information he'd entered. And, as he was using unprotected public WiFi, there was also a risk of the transaction data being intercepted.

What could he have done differently?

Banking should only be done on devices that have anti-malware in place, and always through a secure browser.



Increasingly unwelcome mail

Maria is a psychologist. Every morning, she opens her email to check that her next appointment is confirmed. At the top of her inbox, she sees a message from a social network she uses, asking her to update her password to something stronger. She clicks the link provided, confirms her existing password which is the same, and then replaces every other letter with an asterisk.

Happy that her account will now be harder to hack, she gets back to her inbox and soon forgets the whole thing.

Later, she receives a letter from blackmailers threatening to publish the details of every one of the clients coming to her for therapy.

How did it happen?

Maria was the victim of a phishing scam. Though the site looked just like the one she'd visited thousands of times before, it was just a fake copy. After gaining access to her profile details, they also came across the details of her practice. They tried using the same password, they'd tricked her out of, to hack into her work email. Because she used the same email password for both accounts, they were able to read all her messages and the files attached to them – one of which was a full list of her clients and their contact details.

What could she have done differently?

First, she should have been aware that legitimate sites and organizations will not ask for your details via email. With good security software in place, she would have been alerted to the fact that the site was fake.

Second, she used the same password for both personal and professional use. Varying your passwords is a crucial step in ensuring strong cybersecurity.

True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Get your free trial now >

Learn more at
kaspersky.com/business

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

To learn more about Kaspersky Endpoint Security for Business,
call Kaspersky Lab today at 866-563-3099 or
email us at corporatesales@kaspersky.com.

www.kaspersky.com/business

KASPERSKY lab