SECURITY SPOTLIGHT

FOLLOW THE MONEY:

A Guide to Avoiding Financial Losses in Cybersecurity

KASPERSKY lab

Data breaches cost money. You know that. But how much? And where do most of the costs come from? With the threat landscape changing at a faster and faster pace, it can be hard to know where to put your budget and how to allocate resources. Our research digs deep into the many layers of IT complexity to give you the answers you and your company's leaders need to make the right decisions.

77% Percentage of U.S. businesses that have suffered between 1 and 5 separate incidents of data loss, leakage or exposure in the past 12 months.[1]

FINANCIAL WOES ACROSS THE THREAT LANDSCAPE

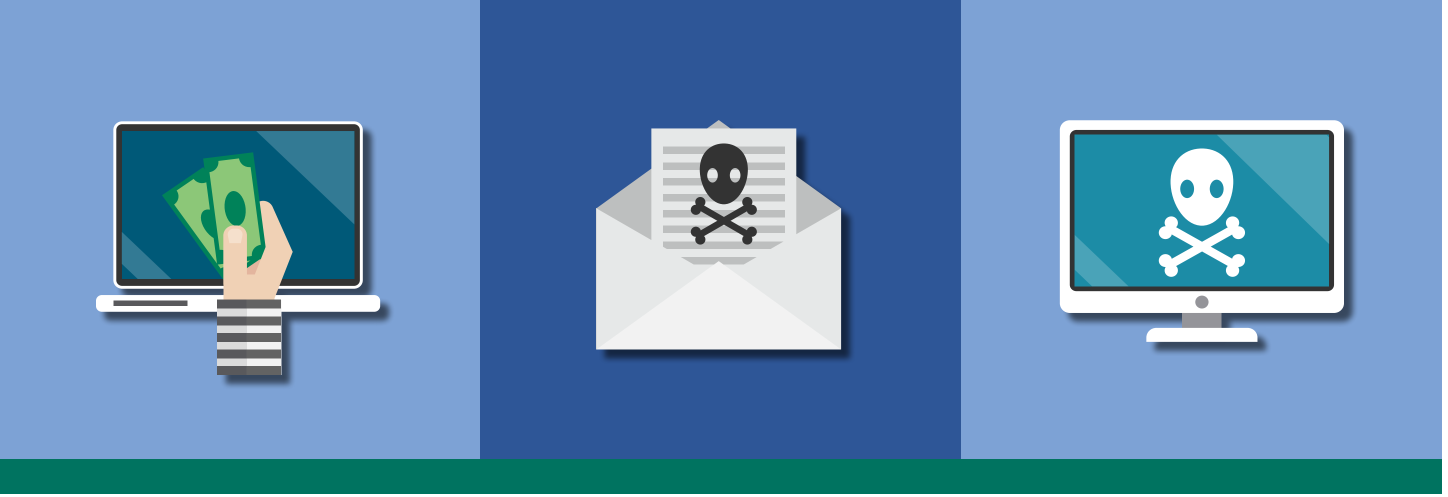
The world of IT security is changing.

With cybercriminals executing attacks whose sophistication is on the same level as nation state attacks, the stakes for businesses are higher than ever before. No longer is it acceptable to have cybersecurity as a line item at the bottom of the budget. It must be a central part of your plan with dedicated IT security staff, education on cybersecurity for employees and the technology to back it all up.

Why? Because the threats are getting more and more expensive. In our *2016 Corporate IT Security Risks Survey* conducted by Kaspersky Lab and B2B International, **57% of businesses now assume that their IT security will be compromised** at some point and that they need to be prepared for these events.

In order for your business to be 100% prepared for an attack, you need to understand what the entire threat landscape looks like and what the greatest threats to your business are.

[1] 1—Kaspersky Lab's *The Financial Impact of IT Security on US Businesses*



Ransomware

Early in 2016, the FBI told CNN that **ransomware was on track to become a $1 billion crime** by the end of year.[2] Cybercriminals have latched onto this form of extortion for its ease of execution and its ability to quickly extract payments from victims. After all, many companies don't expect the sudden shutdown that can occur with a ransomware attack and don't have proper mitigation strategies in place. Cybercriminals know that those with deeper pockets pay up and that many companies panic in the face of the time constraint that comes with most ransom demands.

In the case of cryptomalware, a form of ransomware, the costs can be staggering. **Just one crypto-malware attack can cost a small- to medium-sized business $99,000**. It's no wonder, then, that 49% of SMBs say they consider cryptomalware to be one of the most serious threats that their organization can face.[3]

At Kaspersky Lab, our own solutions protected 443,920 users and corporate customers worldwide from crypto-ransomware and **deprived cybercriminals of nearly $53 million in illegal earnings in 2015**.[4] Cybercriminals go where the money is, and ransomware provides an attractive payout with a low cost of entry.

[2]—Cyber-extortion losses skyrocket, says FBI
[3]—A Single Cryptomalware Attack Can Cost Small- And Medium-Sized Businesses up to $99,000
[4]—Fighting Ransomware: Kaspersky Lab Saved $53 Million for its Clients in 2015

Phishing

Exactly how do cybercriminals get into a company's system? Often, it is by sending employees a phishing email—a fraudulent email that tries to extract sensitive information or launch an exploit by purporting to be from a legitimate source, thereby tricking employees into opening it.

They prey on human fear and emotion by pretending to be a supplier or service provider, sending fake invoices or trying to impersonate a customer. Employees trying to be proactive in their jobs can easily fall into this trap if they are not trained in what to look for and how to avoid the pitfalls.

Data Breaches

One of the biggest ways that the threat landscape has changed is in its scale and scope. Much of today's malware is built specifically to hijack IT systems and make money illegally. As a result, the threats that businesses now face are becoming significantly more complex and more targeted. And the damage they cause is much more likely to be financial, rather than just IT downtime that can be hard to quantify.

According to the *Cisco 2017 Securities Capabilities Benchmark Study*, 23% of organizations that have suffered a data breach have lost business opportunities as a result. Of these, 42% saw a substantial loss of opportunity. In addition, nearly 30% lost revenue as a result of an attack and one in five organizations lost customers.

The financial fallout from a serious data breach can be devastating. According to Kaspersky Lab's own research, **the average financial impact of a serious data breach for an SMB is $149,000. For a large enterprise, the financial impact can run up to $2 million.**[5] This includes additional internal staff time, lost business opportunities, hiring external consultants, PR issues, damage to brand and training for staff. A serious data breach is one that involves a zero day vulnerability, exploits launched through mobiles devices, or a targeted attack. While these are less common, the damage they can inflict on a business can be widespread and long-lasting.

[5]—*Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

$861,000 The average cost of recovery from a single security incident for large enterprise companies.[6]

THE COST TO YOUR COMPANY

Now that you understand what U.S. businesses face across the threat landscape, let's take a closer look at what this could mean for your company specifically.

From a financial perspective, the costs of a security breach can be staggering. For an **SMB, the average financial impact of a single security incident is $86,500. For a large enterprise, the cost is $861,000**.[7] By far, the reallocation of IT staff time represents the single largest additional cost for all size businesses. But the other costs add up, too, such as lost business opportunities and hiring external staff to help mitigate the damage.

In order to prevent these costs, **75% of U.S. businesses expect to increase their IT security spending in the next three years.**[8] Many companies cite the growth and expansion of their own operation as the main need for this increase, but most large enterprises also cite the increased complexity of IT infrastructures as driving this need.

And it's not just protecting your own organization that is important. In fact, **41% of security incidents can be attributed to third-party business partners**.[9] If you are a vendor to a larger enterprise with sensitive information, it is crucial that you can demonstrate to your clients that their company's information is safe with you.

6, 7, 8—Kaspersky Lab's *The Financial Impact of IT Security on US Businesses*
9—*2017 Global State of Information Security Survey* conducted by PwC, CSO and CIO

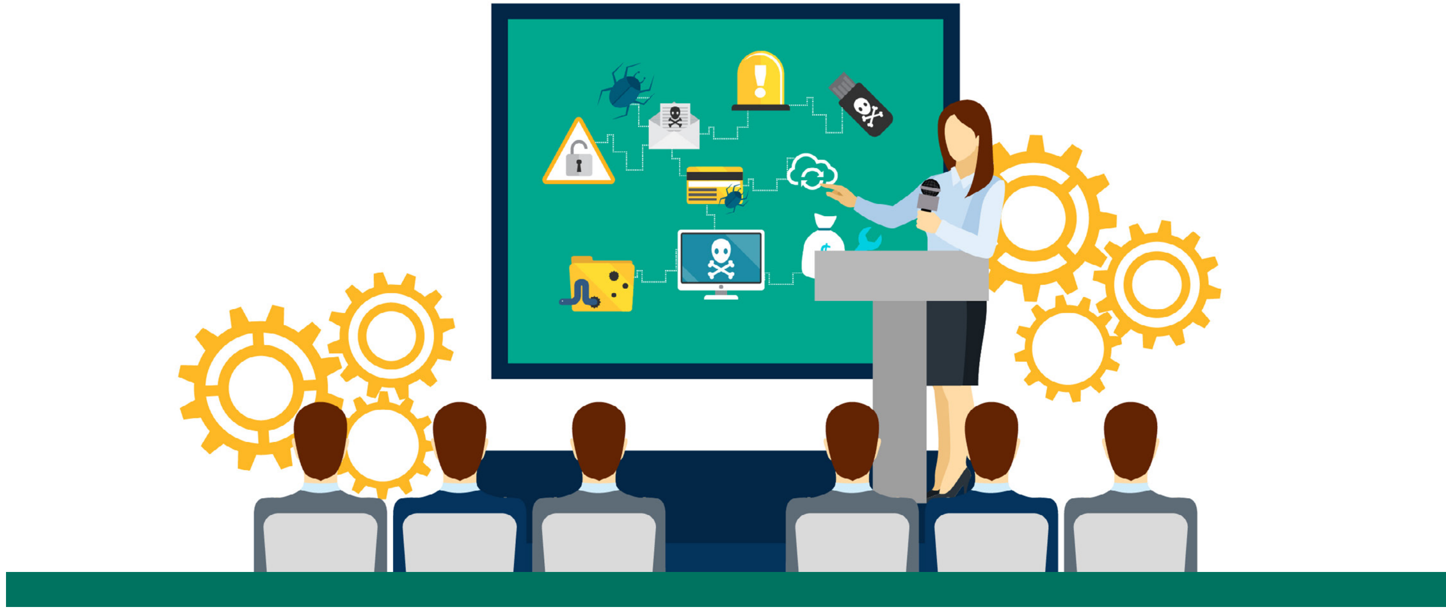
54% Businesses who say that the inappropriate sharing of data by employees via mobile devices is where they are most vulnerable.[10]

EMPLOYEES: YOUR FIRST LINE OF DEFENSE

In building your company's security plan, it's important to take a holistic approach—one that includes a four-part strategy of **Prediction, Detection, Prevention and Response**. While having a multi-layered security solution in place is essential for the prevention of attacks, it is also vital that you are able to predict, detect and respond to attacks. One of the key ways to do this is through employee education.

In terms of cost consequences, **careless, uniformed employees turns out to be one of the highest threats to organizations, second only to malware and viruses** in our broad survey of businesses.[11] This means that having a staff that is informed and aware can save your organization a great deal of money, time and hassle.

With 80% of businesses citing data protection as their top concern and with most of those companies saying leaks from employees is a big factor in ensuring that their data is secure[12], it is essential that companies take the following steps to make sure that their employees act as their first line of defense:



- Ensure that all users know and observe company security policies
- Teach employees about the threats from phishing, social engineering and malware sites
- Instruct all users how to notify IT security staff about all incidents
- Control access to user rights and privileges and keep a record of these privileges
- Scan your system for vulnerable network services and applications that employees may be using without permission
- Update vulnerable components and applications. If there is no update available, then those software and applications should be banned

[10, 11, 12]—*Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

$2 million

For a large enterprise, the financial impact of a serious data breach—such as a targeted attack or a zero day exploit—can run up to $2 million.

EMPLOYEE EDUCATION STARTS AT THE TOP

While leaders of U.S. businesses recognize the need for boosting cybersecurity in the face of increasing attacks, 37% of IT departments say it is still difficult to demonstrate the return-on-investment (ROI) to senior management.[13]

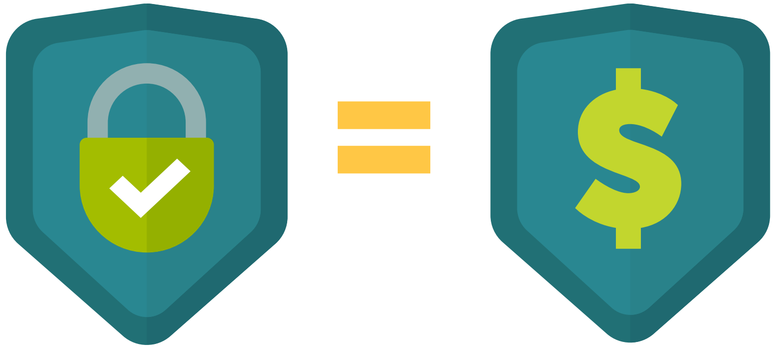
Frequently, cybersecurity is viewed as a technology problem for the IT department to solve, rather than an organizational challenge that every employee needs to participate in. The key to overcoming this challenge is to focus on the dividends that strong cybersecurity investment pays to an organization.

Enterprise or SMB Executives, All Need to Participate

In our Kaspersky Lab and B2B International survey, 20% of large enterprise organizations had suffered four or more data breaches in the past year.[14] As we noted earlier, the average cost of a single security incident for a large enterprise is $861,000. Multiply by numerous breaches over the course of a year, and the costs of not being protected grow exponentially. And if the breach is a serious one—as in the case of a targeted attack or zero day vulnerability—the financial impact can run up to $2 million.

For small- and medium-sized businesses, the average amount spent on IT security is $213,000. With the average cost of an attack at $86,500, this means that **an SMB IT security solution need only to prevent 2.5 attacks before the investment starts paying off.**[15] And if your executives assume that smaller organizations are not a target, think again. According to *USA Today*, 60% of all cybercrime is now directed at small businesses.[16] If your company does business with larger enterprises, then any weakness in your security infrastructure can be a portal through which cybercriminals can access more sensitive data, making your business an attractive target.

The cost-benefit analysis of cybersecurity investments is clear. By allocating an appropriate amount of budget and by helping to foster a culture of IT security right from the top, your company's executives can ensure that they stay true to one of their most important roles—keeping your company safe and secure.



[13], [15]—Kaspersky Lab's *The Financial Impact of IT Security on US Businesses*
[14]—*Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

[16]—Small biz trends: Fasten your seat belts, entrepreneurs

$100,000

Every day that a security breach goes undetected, it can cost large businesses $100,000 on average.[17]

TIME IS MONEY

The old adage that time equals money is true, and nowhere more so than in the world of cybersecurity. The financial costs of data loss incidents goes up quite significantly with dwell time—or the time it takes to detect a breach. If you have sluggish security measures in place, then you could pay dearly.

In the case of cryptomalware attacks, where a single attack can cost SMBs $99,000, detecting it quickly is of the utmost importance. For those businesses that don't catch the infection within a day, 67% report a significant amount of encryption occurring, versus 43% that catch it within a few hours.[18]

In the case of data breaches, the time you take to detect a breach is also critical. For SMBs that catch a breach immediately, the average total financial impact is $28,000. But if they don't catch it for over a week, the financial losses average $105,000. **For large enterprises, those that catch a data breach right away pay roughly $393,000 in related expenses. But wait for over a week, and a large enterprise can pay up to $1.1 million in costs.**[19]

In addition, the damage is not just in dollar amounts. The longer you take to detect a breach, the more records will be compromised. Even a few hours can be incredibly serious. For SMBs that catch a breach quickly, they typically only lose 417 records. But if they don't catch it for over a week, they can lose an average of 70,000 records. **For large enterprises, immediate detection means only 9,000 records lost. Wait over a year, and you can lose an average of 240,000 records.**[20]

Clearly, when it comes to data breaches, the clock is ticking.

[17] —Kaspersky Lab Announces the Availability of its Machine-Readable Threat Intelligence Platform

[18, 19, 20, 21, 22] —*Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Finding the Culprit

For many businesses, the reality of delayed detection is all too real. In our survey, 55% of businesses said that it took them several days to discover a breach. For 26% of companies, detection took weeks or more.[21]

While those numbers are alarming, the way businesses discovered a breach is even more surprising. For those that found out within a few days, 72% of breaches were detected by an external security audit. 65% were detected by an internal security audit, and **55% said that their customers notified them of a breach.**[22] No company wants their clients calling them with that news.

Now imagine what damage occurred for the 10% of companies we surveyed who didn't discover a data breach for up to a year.[23] Our hope is that no company faces that kind of surprise.

[23] —Kaspersky Lab's *The Financial Impact of IT Security on US Businesses*

$99,000 The cost to SMBs of one cryptomalware attack

PEOPLE POWER

Many companies recognize the importance of having IT security technology in place, but it is equally as important to have the people who know how to manage it.

Small- to medium-sized businesses typically only have two dedicated security staff employed. At large enterprises, only 15% of employees in an IT department are dedicated to security. It's no wonder, then, that the the *Cisco 2017 Securities Capabilities Benchmark Study* found that **organizations can only investigate 56% of the security alerts they receive on any given day**.

This shortage has real financial consequences. Our research shows that large businesses hiring outside help pay between $1.2 million to $1.47 million to recover from a cybersecurity incident, compared to those large businesses who have in-house skilled IT security experts to handle a crisis who pay between $100K and $500K.[24]

Almost two-thirds of U.S. companies plan to increase their hiring of IT security specialists within the next three years. Most cite the increased complexity of IT infrastructure as the top driver of this decision. With everything from security issues around the cloud infrastructure to the need to manage business outsourcing, security professionals certainly have a range of issues to manage.

[24] Kaspersky Lab Survey Reveals the Financial Impact of the IT Security Talent Shortage

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY >

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

Learn more at usa.kaspersky.com/business-security

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. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more
about Kaspersky Endpoint Security for Business
and our other IT security solutions and services:
usa.kaspersky.com/business-security
(866) 563-3099
corporatesales@kaspersky.com

KASPERSKY lab

THE POWER
OF PROTECTION