Kaspersky For Business

Missing Pieces: The Five Hidden Vulnerabilities in Your Security Plan

When you're running a business, there are a lot of things to keep track of, not the least of which are your cybersecurity priorities. With a large number of alarming news stories about this topic, it can be hard to keep track of the latest threats and the solutions to them. We'll take a look at the top threats to businesses today and the solutions that will help you stay secure.

46% Careless or uninformed employees contributed to 46% of security events.[1]

Employees and Other Insider Threats

Your employees are your most valuable asset. They are also your first line of defense against cyberattacks. But if that line is weak in any way, a damaging cyberattack can get through your perimeter and steal your data or cripple your business.

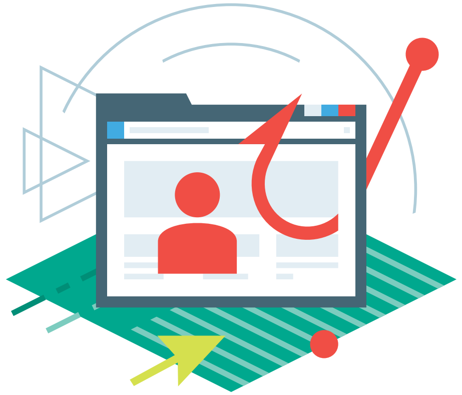
The fact is that careless or uninformed employees are the second most likely cause of a serious data breach, after viruses and malware.[2] Cybercriminals know that they are the path of least resistance to getting at your data, and they exploit this fact all the time. When they are looking for access to your important clients, employee records or financial statements, social engineering tactics that target employees are the path of least resistance towards getting those assets.

Social Engineering

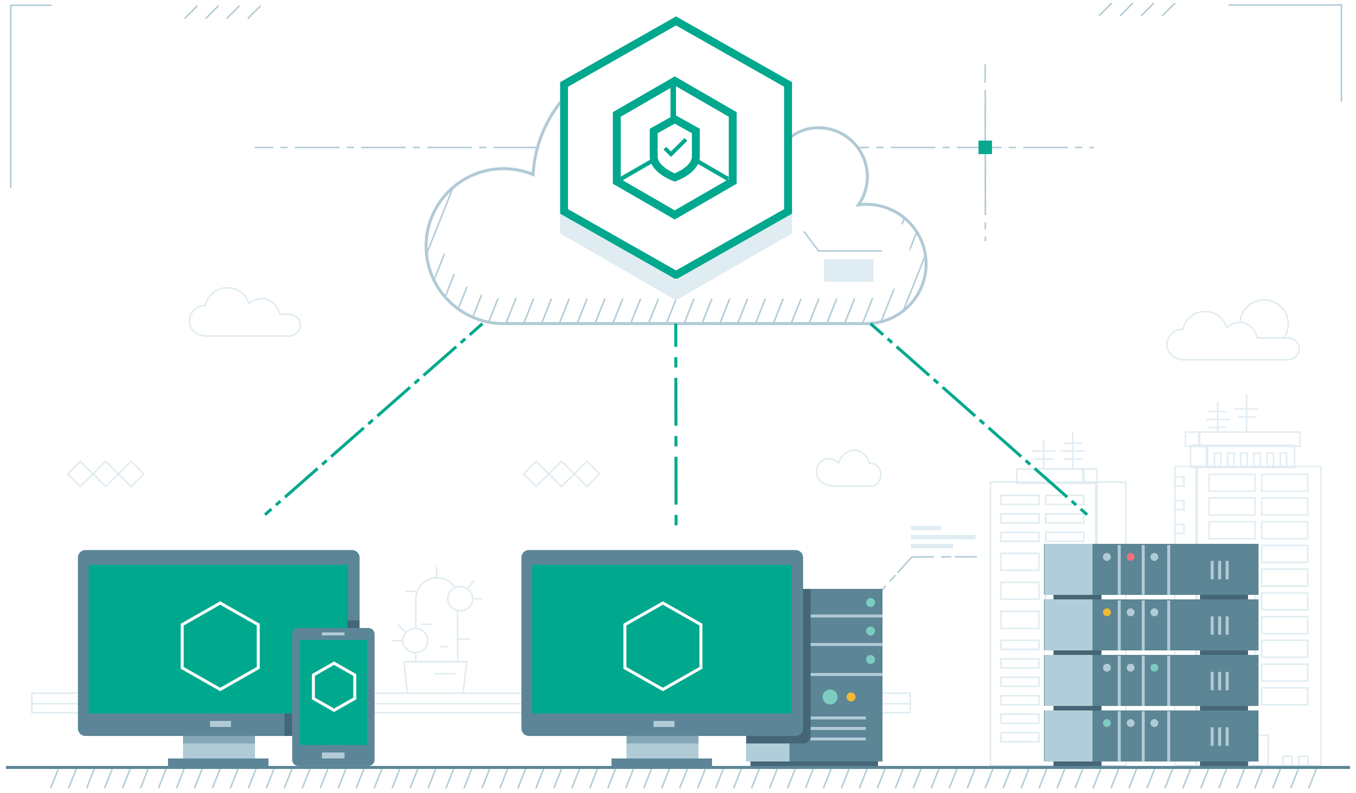
Trust is the currency on which social engineering is based. By sending employees a phishing email and getting them to click on a link or even by calling them up and convincing them they made a big mistake that needs to be corrected, cybercriminals get employees to let them have important information that they shouldn't have.

Employees should be taught to trust their own instincts. If an attachment seems suspicious, don't open it. If a phone call doesn't add up, they should alert someone. If an executive emails them to ask for sensitive information, they should confirm by phone with the person before they send it.

Your employees are the portal through which cybercriminals can gain access to your network. But they can be taught to shut the door and keep it locked.



[1, 2, 3] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International



Security Starts at the Top

Don't assume that executives running your company know what they need to know about cybersecurity. They may sign off on a budget for cybersecurity needs, but this doesn't mean that they fully understand the topic. In fact, since the threat landscape is constantly changing, everyone can use a refresher on their security skills, no matter what position they hold.

Most leaders of organizations recognize the problem, with 52% of companies that we surveyed saying that the biggest weakness in their IT security is the careless actions of employees. 56% of small- and medium-sized businesses and 66% of enterprises have invested in IT security awareness training in the past year.[3]

Much of this issue comes down to creating a culture of cybersecurity, and that starts at the top. If leaders make it a priority, so will everyone else in the business. If they show up to training sessions, reinforce the message in communications to employees and insist on properly vetting third parties, it will go a long way towards defending your company from threats.

$163,000	**Cost of an attack to SMBs when it resulted from the actions of outside contractors with access to their network.**
$1.5 million	**Cost of an attack to large enterprises when it resulted from the actions of outside contractors with access to their network.[4]**

Third Party Security

Our research shows that four out of five business applications, on average, are supplied either through private cloud or hosted remotely as part of a SaaS offering, including email, HR management and finance and accounting systems.[5] Mobile devices are a particular problem for small- and medium-sized businesses, and the growing Internet of Things is seen as a big trend that will affect IT security.

Many companies understand the potential scope of this problem. In fact, 50% of those we surveyed said that they are more concerned with the security of third-party infrastructure than their own. Nearly 44% say that they are becoming too reliant on third parties for critical resources, noting that if the provider's network is down, they cannot do their work.[6] Without a clear plan in place to deal with incidents, many businesses are vulnerable. With 78% of businesses over 50 employees already making use of at least one form of cloud services, you can see how widespread the problem can be.[7]

As a result of this, more and more businesses are demanding increased security from their vendors and third-party solutions. In fact, 24% of companies say they will be increasing their IT security spending due to demand from customers.[8] Clearly, the market is starting to understand that no company is an island. With third-party partners acting as a major source of security incidents,[9] companies are starting to take notice and make it a key part of whom they do business with.

The main takeaways are clear. If you are an organization that does business with third-party partners of any kind, you need to vet them for solid security practices. If you are a vendor, SaaS solution or cloud provider, you need to be able to prove that you are able to secure your clients. It's that simple.

[4, 5, 6, 7, 8] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International

[9] *2017 Global State of Information Security Survey conducted by PwC, CSO and CIO*

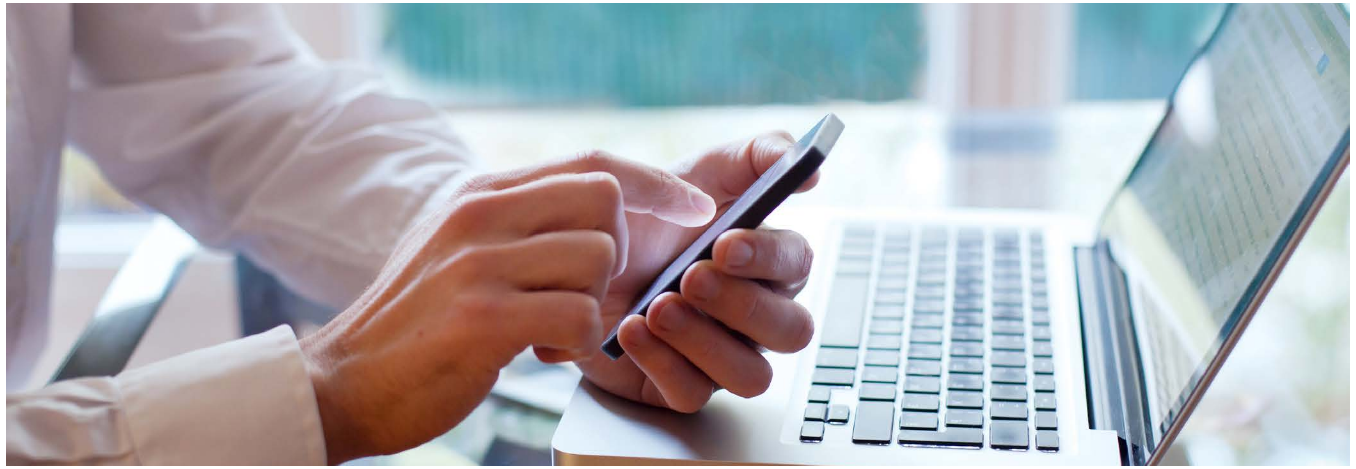
47% **Businesses who say that the inappropriate sharing of data via mobile devices is a major security concern[10]**

BYOD Security

In our survey of more than 5,000 business leaders, 47% said that the inappropriate sharing of data via mobile devices is a major security concern that they deal with often. 31% have experienced the inappropriate sharing of data via mobile devices in the past year. For large enterprises, the stakes are especially high, with costs of a data breach averaging $1.7 million when the attack comes from exploits or loss of mobile devices.[11]

Clearly, the issue is one that companies of all sizes deal with and one that has far-reaching consequences.

Implementing a strong Bring Your Own Device (BYOD) program starts with getting employees invested in mitigating losses and protecting data. If employees understand that your policies are there for a reason and that upper management supports them, it will go a long way towards getting people to follow them.



Add to that a strong mobile security solution that runs on all devices, and you will be doing everything you can to make sure that your data is secure and your company is safe. When selecting a mobile security solution and implementing it, we recommend that you look at the issue from four angles: users, devices, programs and infrastructure.

Users. Knowing how people use their devices and why is key to determining an effective BYOD policy. Someone in Finance may need to access a different set of data than someone in Sales. Ask them, how do you commonly use your devices? What data do you need to access? What privileges are you comfortable granting? What will you do if a device is lost or stolen?

Devices. The devices you allow in your organization will determine a large part of your security policy. Make sure they reflect not only employees' needs and wants but also what customers will probably ask for. Find out, what kind of devices do they need to use the most? How will each mobile devices be deployed? What security constraints do you need to enforce in order to comply with your organization's business needs?

Programs. It's important to strike a balance between what employees want and what keeps your organizations secure. Keeping out some apps and programs entirely will be a necessary part of your security structure. What apps and programs do employees need to do their jobs? Which ones do customers need? What are risky programs or apps that you want to block?

Infrastructure. Change is one of the only constants on the IT landscape. Make sure you build enough flexibility into your plan to account for inevitable growth and change, both within your organization and in the world of technology. Does your IT department have the bandwidth to support mobile needs? How can you keep your infrastructure flexible enough to allow for future technology?

[10, 11] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International

$117,000 Average financial impact of a data breach for SMBs in North America.

$1.3 million Average financial impact of a data breach for large enterprises in North America.[12]

APTs: The 1% of Threats that Cause the Most Damage

Advanced Persistent Threats (APTs) are complex attacks, consisting of many different components. Using penetration tools, such as spearphishing messages or exploits, network propagation mechanisms, spyware, and rootkits or bootkits to conceal their presence, APTs are designed with one objective in mind: gaining undetected access to sensitive information.

Why do we call them Advanced Persistent Threats? APTs are "advanced" because the tools used in these attacks are more sophisticated than those usually used by cybercriminals. They are "persistent" because once an organization is breached, it can remain in the system for months or even years. In fact, according to a study by HP and Mandiant, the median amount of time before a company detects a data breach is 205 days, leaving cybercriminals with months of access to sensitive data before they are discovered.

[12] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International

Because APTs make up just 1% of the threat landscape, they are rare, but they are the threats that can cause the most damage and be incredibly costly to any company. There are several steps you can take to arm yourself against these pernicious threats:

Install a multi-layered security solution. APTs are sophisticated, and they are specifically designed to break through firewalls, penetrate servers and bypass security programs. Remember, the data they are after is highly valuable, so spending the time to develop malware that is highly advanced is worth the effort to cybercriminals. By implementing a multi-layered security solution that can catch these highly targeted attacks, your organization and its important data will be much safer.

Threat intelligence. The threat landscape is a moving target with cybercriminals looking for new ways to thwart systems and trick employees. Staying on top of it all is a huge task, so it helps to have a partner who can give you the information you need to know. Studying APTs is complex and time-consuming, so we recommend partnering with a knowledgeable organization that issues reports from its findings. At Kaspersky Lab, we dig into large amounts of data to look for languages used in the code, time when the malware was compiled, IP addresses and who is being targeted, among many other factors. All of this information forms a matrix that we can follow to advise our clients on where cybercrime is moving and what type of data to protect.

59% of businesses now assume that their data will be compromised at some point. Among businesses that have suffered a targeted attack, 67% feel this way. When businesses are targeted by one of these advanced attacks, they don't soon forget it, and they look for ways to be prepared with the tools and threat intelligence that will secure them.

$102,000	Cost to SMBs if they take more than a week to discover the ransomware infection.
$1.2 million	Cost to enterprises if they take more than a week to discover the ransomware infection.[13]

Ransomware

With stories of ransomware hitting the news in recent years, many companies are aware of the issue. But many also don't know how to protect against it.

The important thing to remember is that time is of the essence. For businesses that don't catch a ransomware infection within a day, 74% report significant amounts of encryption occurring versus 52% that catch it within a few hours. Recovery is also less successful if detection is not within hours with 36% reporting losing significant numbers of files entirely if it takes a day or more to detect. Since 34% of businesses say it took a week or more to recover their data, we can see what a powerful foe ransomware is to the business world.[14]

[13, 14, 15] *Global IT Security Risks Survey 2017* from Kaspersky Lab and B2B International

Many think that paying the ransom is the solution to this problem. But among the 36% of businesses who paid the ransom that we surveyed, 1 in 5 did not get their data back.[15] In addition, paying the ransom does not necessarily mean getting your data back. It should come as no surprise that cybercriminals sometimes lie. Many of them who say they can help get your files back never had the decryption key in the first place.

The real solutions to ransomware involve preparing on multiple levels:

- **Back up your files regularly.** The only way to ensure that you can immediately handle a ransomware attack is to implement a regular backup schedule so that your company can get access to the files it needs without dealing with the cybercriminals. Your backup should have certain restrictions, such as read/write permissions without an opportunity to modify or delete the files.
- **Check your backups.** There are times when something can damage your files. Be sure to check regularly that your backups are in good shape.
- **Regularly update your operating system.** Cybercriminals tend to exploit vulnerabilities in software to compromise systems. 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.
- **Use a robust antivirus program to protect your system from ransomware.** Our Kaspersky Lab products employ a multi-layered system of defense that checks malware from many different angles to ensure that it does not corrupt your system.

If ransomware does hit:

- **Cut off your internet connection immediately.** If you discover ransomware, shut off your internet connection right away. If the ransomware did not manage to erase the encryption key from the computers in question, then there is still a chance you can restore your files.
- **Don't pay the ransom.** If your files become encrypted, we do not recommend paying the ransom unless instant access to some of your files is critical. Each payment made helps the criminals to prosper and thrive to go on to build new strains of ransomware.
- **Try to identify the malware.** If you are hit by ransomware, try to find out the name of the malware. Older versions of ransomware used to be less advanced, so if it is an earlier version, you may be able to restore the files. Moreover, cybersecurity experts, including Kaspersky Lab experts, collaborate with law enforcement to provide file restoration tools online and, hopefully, detain the adversaries. Some victims are able to decrypt the files without having to pay the ransom. To check whether that's possible, visit kaspersky.com

How do Kaspersky Lab products protect your company?

While there are many things you and your users can do to prevent attacks, implementing a multi-layered security solution is still the best defense against these sorts of attacks. Kaspersky Lab's products secure your organization through layer after layer of countermeasures that ensure that you are protected.

Our technology uses a range of sophisticated behavioral technologies to discern suspicious patterns, block malicious activities and roll back any harmful actions, including malicious file encryption.

Workstation Protection

Vulnerability Assessment And Patch Management

Vulnerabilities within any of the applications and operating systems running on your devices can provide entry points for ransomware. Our automated Vulnerability Assessment and Patch Management tools scan your systems, identify known vulnerabilities and help you to prioritize and distribute the necessary patches and updates so that known security vulnerabilities can be eliminated.

Anti-Phishing

Because phishing emails are usually the starting point for many ransomware attacks, Kaspersky Lab's anti-phishing technology uses a multi-layered approach to protect against infiltration. First, it checks sites with the product's local anti-phishing databases on the user's device. Next, it checks URLs of sites against Kaspersky's own vast, continually updated database of phishing sites, which are collected through Kaspersky Security Network. When a new malicious URL is detected on the computer, information about this threat is made available from the cloud database within 15-30 seconds of detection. Finally, our heuristic analysis is an intelligence system that looks at dozens of phishing symptoms and compares it with other indications, classifying them based on known modern phishers' methods and the vast Kaspersky Lab database of already detected phishing sites.

Heuristics

Heuristic analysis provides proactive protection from threats that can't be detected using signature databases. Kaspersky Lab's heuristics enable the detection of new malware or unknown modifications to known malware. Static analysis scans code for signs of suspicious patterns associated with malware, while dynamic analysis examines the machine code the file might try to execute.

Default Deny

Increasingly viewed as the most effective security posture to adopt in the face of ever-evolving, advanced threats, Default Deny simply blocks all applications from running on any workstation unless they have been explicitly allowed by the administrator. Since most malware is delivered as an executable file that cannot be found on any whitelist, organizations that adopt this approach can thus prevent any malicious file from executing without really needing to know what those files actually are. Default Deny means all new, file-based malware varieties are automatically blocked, even for targeted attacks.

System Watcher

System Watcher monitors applications and processes activity to discern behavioral patterns, relying on behavioral stream signatures that look at sequencies of actions, rather than just one isolated action. Malicious actions and destructive behavior patterns suggestive of malware are blocked.

Automatic Exploit Prevention (AEP)

As part of System Watcher, this technology specifically targets malware that exploits software vulnerabilities. AEP acts like a safety net, an extra layer of security that complements Kaspersky Lab's other technologies.

Rollback

Our crypto-malware countermeasure subsystem negates the consequences of crypto-attacks by making local, protected backup copies of user data files as soon as they are affected by a suspicious program, returning user data to its original preserved state.

Server Protection

Application Launch Control

Application Launch Control prevents unapproved applications from launching and spreading malware right from startup.

Anti-Malware With Kaspersky Security Network Integration

Our anti-malware protection draws on our global network of sensors to anticipate the latest threats, giving our technology a worldwide perspective on evolving threats. This intelligence is then applied to our technology in order to protect your infrastructure before the attack ever reaches your server.

Anti-Cryptor

Our Anti-Cryptor technology monitors the server for signs of corruption, cuts the infected workstation's access to the server for 30 minutes, and alerts administrator to the infection.

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.

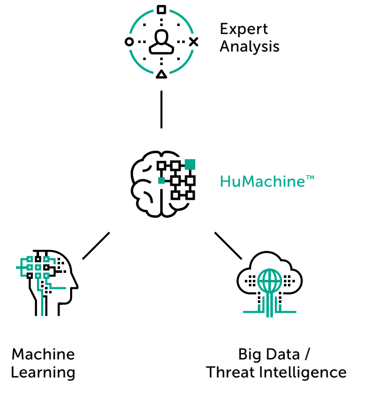
About Kaspersky Lab

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 about cybersecurity: **www.securelist.com**

www.usa.kaspersky.com
#truecybersecurity

Kaspersky Lab, Inc.
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com


Expert Analysis
HuMachine™
Machine Learning
Big Data / Threat Intelligence