KASPERSKY lab

TAKE IT TO THE BOARD

What your Board of Directors needs to know about cybersecurity

$551,000 Average cost of a serious data loss event for Enterprises

60% Number of businesses that find their ability to function severely impaired[1]

Forty-eight percent of large organizations report that their Board of Directors is actively involved in the overall security strategy of their company.[2]

As a leader in your IT organization, you understand that cybersecurity is an issue that increasingly makes its way up to the C-suite. But how do you answer their most pressing questions?

How do you present solutions that strike the balance between security and efficient operations?

How do you make the most compelling case for more resources to protect your enterprise?

With the average cost of down-time following an attack at $1.4 million[1], the stakes are high. And as more and more data moves outside of your organization through mobile working and the sharing of information, helping your Board of Directors to understand the risks involved is imperative.

Looking at topics from the need to educate employees to how to manage technology sprawl, our research breaks through some common myths of building an IT security plan. This data can help you to address some commonly held misconceptions and to focus on the high value points that will make the best case to your Board of Directors for greater allocation of resources and budget.

1. Kaspersky Lab "Global IT Security Risks Survey 2015"
2. The 2016 Global State of Information Security Survey, in partnership with PwC, CIOmagazine, CSO, October 2015

73% Organizations that have had an internal security incident in 2015. Top threats came from software vulnerabilities and accidental actions by staff, including mistakenly leaking or sharing data.[3]

Myth #1: Employee education is a nice add-on item.

If only it were that simple.

The fact is that 34% of current employees are the likely source of security incidents, according to a survey of current executives of large enterprise organizations.[4]

Human beings are still the weakest link in the security chain. Whether it's intentional or unintentional, employees can leak sensitive data from your organization, leaving your IT department scrambling to mitigate the damage.

Many employees have a false sense of security around IT issues, believing that they do not play a role. Helping them to understand the dangers of phishing, spearphishing and social engineering and how they can help to stop those threats will benefit your organization by shoring up an important first line of defense against hackers.

Among enterprise companies, there is an increasing understanding that internal IT departments alone cannot educate employees, which is why 42% now use IT security education services.[5] And because threats keep evolving, cybersecurity education is an ongoing process.

3, 5. Kaspersky Lab "Global IT Security Risks Survey 2015"

4. The 2016 Global State of Information Security Survey, in partnership with PwC, CIOmagazine, CSO, October 2015

People play a major role in securing data. As part of a well-planned budget, employee education is a preventive measure that can save enterprises much more than the initial cost of investment by helping to protect stored information, reduce disaster recovery costs and preserve brand reputation.

90% Number of businesses with over 250 employees that would pay for greater security if it meant more secure financial transactions.[6]

Myth #2: Security is an internal issue.

Only 40% of large enterprises feel very confident that their partners' and suppliers' information security activities are effective[7], and 37% of them are concerned that their SaaS providers' platforms are not secure.[8]

With greater awareness of widespread and high profile security incidents, expectations are higher than ever that partners and vendors will provide a secure environment for transactions. The fact is that many companies are not keeping up with these expectations.

And as more and more organizations report security incidents in which their partners were implicated, it's clear that third-party vulnerabilities are not only an emerging concern but also a possible cost.

If you are a third party vendor that can demonstrate strong capabilities in this area, it will be a compelling selling point when negotiating contracts. More important, it will save your company the mitigation, disaster recovery costs and reputational damage that can do much greater long-term damage.

6, 8. Kaspersky Lab "Global IT Security Risks Survey 2015"

7. The 2016 Global State of Information Security Survey, in partnership with PwC, CIOmagazine, CSO, October 2015

No company is an island. Each one is dependent upon vendors, suppliers and partners to hold up their end of the security bargain. In fact, more and more expect it.

36% Information workers who have had a mobile device exploited.[9]

Myth #3: Endpoint protection is a set point on the IT landscape.

With the average information worker using three devices, securing all of your endpoints is becoming a greater challenge that encompasses desktops, servers, and mobile devices at the minimum.

Add to this the fact that more and more data is moving outside of your organization every day, and you have the challenge of trying to fit together the many moving parts of information security into one viable solution.

So, how do you tackle cybersecurity challenges when so many of your endpoints are are moving outside your perimeter? More important, how do you communicate to executives that this is a facet of cybersecurity that affects every corner of your organization?

Start with planning for complexity. Knowing that your organization will be adding people and devices over the next year, all C-level executives should understand that a truly effective cybersecurity platform is one that includes plans for growth and leaves room for flexibility.

With 21% of organizations having lost sensitive data from internal threats in the past year,[10] securing your organization beyond the desktop and server is an essential component of any enterprise security budget.

9. The 2016 Global State of Information Security Survey, in partnership with PwC, CIOmagazine, CSO, October 2015

10. Kaspersky Lab "Global IT Security Risks Survey 2015"

Complexity is the enemy of security, but planning for complexity is a simpler solution than mitigating data loss.

THE BOTTOM LINE FOR THE BOARD

90% Organizations who have experienced some form of external threat.[11]

Myth #4: One attack cannot bring down a whole system.

All it takes is one weak point. That's all cybercriminals are looking for in order to gain access to your organization's most sensitive data.

Sophisticated threats are constantly emerging, and cybercriminals are developing more innovative techniques to circumvent security technologies. Some of the most insidious of these attacks are APTs, which comprise 1% of the threat landscape but which are among the most dangerous threats to any enterprise organization.

Defending against Advanced Persistent Threats has become a priority for most enterprises—enough so that 60% of large enterprises globally will utilize commercial threat intelligence services to help inform their security strategies by 2018.[12] In order to combat APTs, your IT department must engage all of the solutions at its disposal to defend against this growing threat.

At the heart of this defense is building a strong data center to support your vital business processes. When a single network worm can take your whole system offline, you need a data center that combines the best security to defend against the most serious threats with the flexibility to meet the performance needs of your organization.

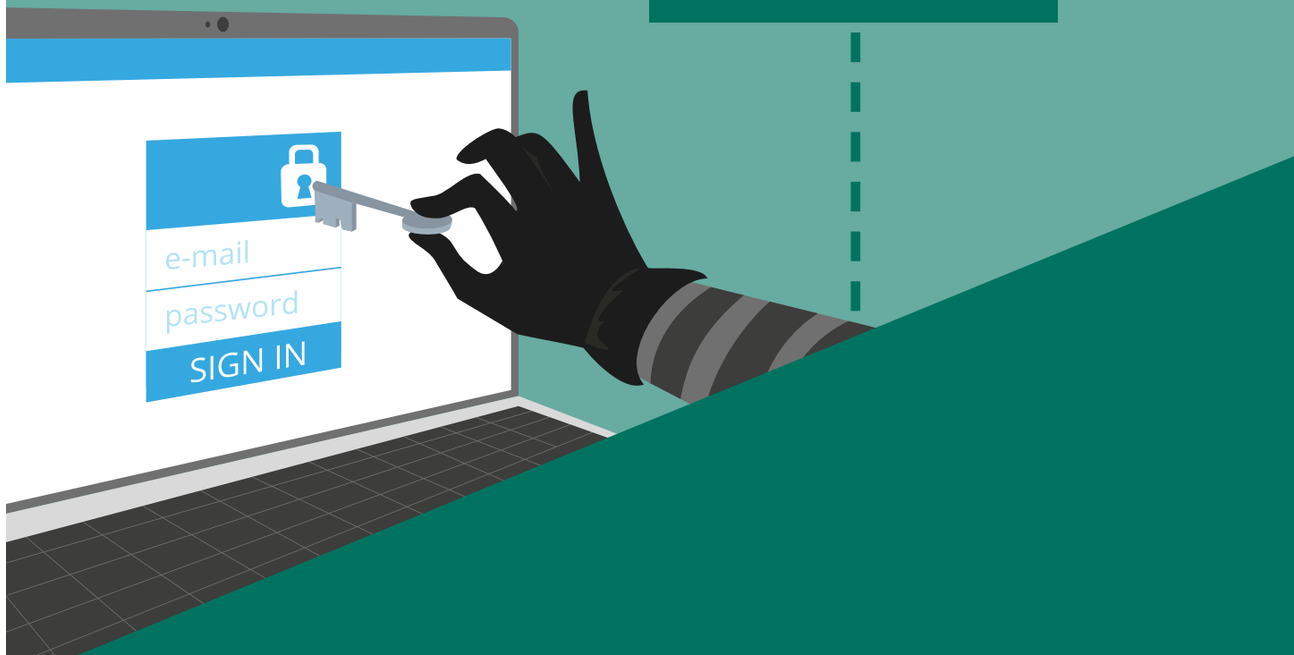
With a planned solution that eliminates all the identifiable gaps, you can stay ahead of the known, unknown and advanced threats that comprise the greatest threats to your organization.

11. Kaspersky Lab "Global IT Security Risks Survey 2015"

12. Kaspersky Lab "Security Intelligence Services" report

Rigorous security that keeps pace with the latest threats is a necessity. This means employing a comprehensive enterprise security solution that addresses known, unknown and advanced threats.

THE BOTTOM LINE FOR THE BOARD



$942,000 Average enterprise cost of a data breach that involved virtual environments—a figure that is more than double the $454,000 average cost of a breach not involving a virtual environment.[13]

Myth #5: You can protect your virtual infrastructure with existing, traditional security software.

When rolling out a virtual infrastructure, the issues can be highly complex and difficult to grasp. In fact, only one-third of organizations possess strong knowledge of each solution available to them for securing a virtual environment.[14]

While 64% of IT professionals say that security should be one of the first considerations when putting in a virtual infrastructure, 43% agree that security poses a significant barrier to virtualization.[15]

Why all the confusion? Where's the disconnect?

It all stems from a misconception about what kind of technology is appropriate for a virtual environment. Multiple devices, multiple clouds and multiple applications can leave systems open to vulnerability, while also adding complexity that traditional security solutions were not designed to deal with. Add to that the growing amount of data stored on virtual servers, as well as virtual-specific malware, and you have a whole new landscape of threats. By implementing a virtual security solution, such as Kaspersky Security for Virtualization (KSV), your business can address those threats with technology that supports the unique needs that your virtual infrastructure requires.

With the costs of a virtual data breach running double the costs of a data breach in a traditional environment, it's clear that a traditional approach for virtualization security is a risky proposition that most enterprises should not be taking.

13, 14. Kaspersky Lab "Global IT Security Risks Survey 2015"

15. Kaspersky Lab "Security for Virtualization"

The "softer" costs of an attack on your virtual infrastructure can have a more significant long-term impact than the immediate direct costs. By implementing a security solution that is designed to address the specific threats to a virtual environment, you can protect your business from the legal fees, brand damage and business continuity costs that can result from a breach to your virtual environment.

THE BOTTOM LINE FOR THE BOARD

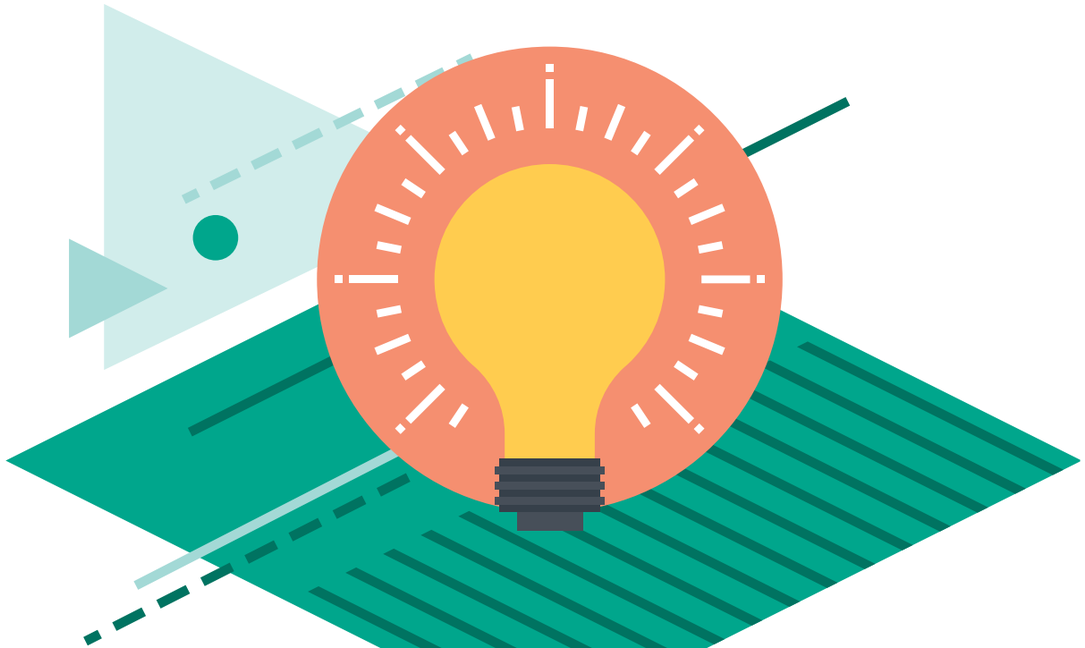
Myth #6: You can do it alone.

The threat landscape for enterprises is constantly changing, and a one-size-fits-all solution is no longer sufficient to protect organizations against growing and persistent threats.

Whether the issue is APTs, virtual systems, or educating your employees, IT security decisions have never been more complex. Very often, organizations can only see the value of security solutions in hindsight. This blind spot often leads to cybersecurity being an expense that is separate from the rest of the IT infrastructure—a very expensive afterthought.

Not even the largest enterprise organizations can defend themselves without solutions that encompass fully integrated software, employee engagement and understanding, and the steadfast participation of their Board of Directors.

Supported by solid data, a well-planned budget and the commitment of your Board of Directors to fiscal and personal responsibility, your enterprise can successfully navigate the hazards that threaten your organization.



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