IT SECURITY BY THE NUMBERS: CALCULATING THE TOTAL COST OF PROTECTION
Cloud computing... mobile devices... web applications... virtualization. It seems there are backdoors into your systems from every direction. And that’s before you’ve even considered the threat presented by the very applications your end users need to get their jobs done. Third-party applications accounted for 87 percent of all vulnerabilities in 2012.¹

Or how about the 315,000 new malicious programs Kaspersky Lab detects every day, or the 132 million applications at risk we recorded in 2012?² Researchers at Purdue University found that malicious software introduced via a mobile or other device can spread to 500,000 devices in just 100 seconds.³ In fact, for every 25 percent increase in functionality, there’s a 100 percent increase in complexity, also known as “Glass’s Law of Complexity.”⁴

---

The Slower Pace of IT Spending

Just keeping up with the patches and critical updates for all the different endpoints, devices, and applications can be a full-time job. Unfortunately, there may not be a person to do the job on even a part-time basis for many businesses.

While malware has exploded in recent years (along with the technologies it can exploit), the same cannot be said for IT security spending:

- PriceWaterhouseCoopers reported a decline in the employment of information security staff between 2011 and 2012.\(^5\)
- 58 percent of companies admit their IT security is under-resourced in at least one area of staff, systems, or knowledge.\(^6\)
- 40 percent of businesses report feeling unprepared for the threats facing them.\(^7\)

---


\(^6\) Kaspersky Lab, “Global IT Risks Survey 2012.”

\(^7\) Kaspersky Lab, “Global IT Risks Survey 2012.”
Regrettably, the cybercriminals aren’t having such a hard time and the constantly evolving threat landscape is flourishing. Today’s malware writers are financially motivated – and often backed by organized crime. With credit card details selling for mere pennies online, the big fish have followed the money into intellectual property, cyberespionage, and competitive intelligence.

The bad guys often purchase software elements on the black market to build their own malware. “[It’s] easy to find people on the Internet who will develop malicious code to order – they usually offer their services on public hacker forums frequented by cybercriminals and scammers.”

It doesn’t matter what size your business is either. If it’s of value to you, you can bet it’s valuable to criminals, too. Indeed, small and mid-sized businesses are increasingly being targeted because they represent a backdoor into larger enterprises and require fewer resources than do attacks against more sophisticated corporations.

Worms, viruses, Trojan horses, phishing attacks, spam … they’re all still out there – but criminals are developing new ways of using them. The bad guys now blend them into advanced persistent threats designed to target and exploit specifically identified weak spots in your business.

The solutions designed for yesterday’s malware don’t cut it in today’s environment. There’s simply too much going on. Signature-based antivirus software at the email gateway misses zero-day attacks, rootkits, botnets, drive-by downloads, and spyware. To fight today’s threats, businesses need sophisticated anti-malware technologies that protect the entire dynamic IT environment. It’s not just the technology that needs to change, though; the perception of anti-malware as a checkbox, commodity solution is yesterday’s thinking.

---


9 Threatpost Spotlight Series, 2012-2013.

“These types of attacks against smaller, resource-strapped organizations are most prevalent, and the most profitable.”
Choosing Smart Protection

As Lysa Myers, director of research at West Coast Labs, put it: “Anti-malware software is only as good as its research and support departments. They are vital in order to have excellent response times to new threats and to provide top-notch customer assistance. Plus, it needs to cover more than the desktop. As the focus in corporate networks shifts away from the desktop to mobile, and virtual computing resources, security software needs to protect these environments too.”

Protection needs to be intelligent, too. “Protection is more than current malware detection capabilities, it’s also about the extent of a vendor’s product research and development strategy that anticipates threats and trends to ensure proactive network protection,” said Myers.

Some points worth considering:

- Choosing anti-malware – or any essential software – is no longer a price-based decision. If price were all that mattered, every company in the world would be doing just fine using free anti-malware software.

- Choosing the market leader carries no guarantees either. The strengths that drove that provider to the top of the market aren’t necessarily the capabilities that will protect your business today and into tomorrow as your infrastructure changes.
The Total Cost of Protection

For every new threat discovered, another security company comes on the scene, offering you the latest and greatest antivirus software, sometimes for free. But is it really such a bargain?

It’s time to look beyond cost and start considering value. At Kaspersky Lab, we recommend a new approach to evaluation of anti-malware solutions: Total Cost of Protection.

The Total Cost of Protection is the sum of all the costs associated with anti-malware deployment, including:

- Protection
- Performance
- Management
- Support
- Price

If any one of these elements is out of line, there’s an increase in total costs. Have you ever considered whether it’s costing you more to run your anti-malware solution than it did to buy it? Let’s take a closer look.

Victims Keep Paying

The cost of cyberattacks for businesses

How big is the bill facing a company hit by a serious cyberincident?

Enterprise–level companies

- $158,000
- $13,000
- $23,000
- $858,000
- $661,000
- $984,000
- $1,670,000
- $2,400,000

SMBs

- $11,000
- $5,000
- $457,000
- $258,000
- $26,000

**such as Kaspersky Endpoint Security for Business

**such as Kaspersky Targeted Solutions for corporate IT-infrastructure

Source: Global Corporate IT Security Risks 2013, B2B International

Reasons for security incidents & measures to avoid them

1. Malware attacks
2. Vulnerabilities in software
3. Accidental leaks or data sharing by staff

Top 3 causes of serious data loss:

1. Malware attacks
2. Vulnerabilities in software
3. Accidental leaks or data sharing by staff

To do list:

- Appointing new IT Security personnel
- IT Security training for existing personnel
- Proper protection solution
- Targeted solutions for potentially vulnerable parts of infrastructure (mobile devices, mail servers, virtual servers, storage, etc.)

The cost of different types of attacks

<table>
<thead>
<tr>
<th>Type of attack</th>
<th>Enterprise / SMB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted attack</td>
<td>$1,538,000 / $71,000</td>
</tr>
<tr>
<td>Network Intrusion</td>
<td>$990,000 / $51,000</td>
</tr>
<tr>
<td>Fraud/Deliberate leaking</td>
<td>$984,000 / $51,000</td>
</tr>
<tr>
<td>Phishing</td>
<td>$858,000 / $37,000</td>
</tr>
<tr>
<td>Exploits</td>
<td>$661,000 / $61,000</td>
</tr>
<tr>
<td>Dos/DDoS</td>
<td>$527,000 / $58,000</td>
</tr>
</tbody>
</table>

The cost of cyberattacks for businesses

How big is the bill facing a company hit by a serious cyberincident?

10 "Global Corporate IT Security Risks Survey 2013."
Anti-malware exists to protect your IT environment from multiple threats. Is your solution living up to its name? Poor or inadequate protection stems from:

- Infrequent updates, leaving systems vulnerable.
- False positives on virus detection, wasting IT resources addressing imaginary issues.
- Faulty updates that cause system crashes.
- Failure to detect malware and prevent infections.
- Failure to clean up and remove infections, requiring manual intervention.

How effective is your current software at protecting you from malware? Does the vendor invest in research into protection for new technologies?

Poor quality or outdated anti-malware software can end up costing you more in the long run; whether it’s the cost of data loss, reduced employee productivity, wasted or poorly managed IT resources, or the long-term effects of the reputation damage that follows a breach, low-grade security often comes at a very high price.
The Performance Trickle-Down Effect

Contrary to what you might think, IT security and system performance are not mutually exclusive. Most IT managers and end users can relate to the bloatware experience, where updates and scans soak up processing power to the point that systems are as good as unusable.

System scans, signature updates and upgrades are vital to effective IT security. But if productivity grinds to a halt while your chosen solution does its thing, you’ve dramatically increased the Total Cost of Protection.
Bad Management

It’s easy to be blown away by features and technologies – but who’s going to manage everything? Cumbersome, distracting, non-intuitive, and resource-sapping bells and whistles just add to your costs in the long term – or become expensive white elephants, as hard-pressed IT staff switch them off in order to get things done. Poor management means:

- More hours to finish the same job.
- Increased time and money spent on training.
- Complexity leads to mistakes, which in turn can result in protection gaps or poor policy enforcement.
- Complexity confuses: lack of clear reporting or visibility leaves you vulnerable.

Reducing the number of management consoles reduces the risk of cybercrime for your business. Management should be simple, easy to use, yet granular and powerful enough to address risk.
Support is a critical component of any deployment – yet it’s often the most overlooked aspect of the evaluation process. Toll-free numbers are only as good as the human answering the call. And does that include after hours or weekends? Are there additional fees involved for setup, troubleshooting, and ongoing consultation? And if you’re a smaller business, can you expect the same high levels of service received by your chosen provider’s bigger clients? These are all very important factors in assessing the Total Cost of Protection.

Poor support costs you time, money and lost productivity – often in the name of resolving simple issues. Support is too critical to neglect. Research shows that IT security staff already feel under-resourced. If they don’t have the time and expertise to handle the security challenges, you need to be sure that your anti-malware vendor is available and equipped to provide that support.
Beware the Bitter Aftertaste of a Sweet Deal

Everyone is looking for a good deal, but as we’ve seen, evaluating security solutions based on price alone can mean you get more than you bargained for on the Total Cost of Protection front.

As with most things in life, if it seems too good to be true, it probably is. That free solution is tempting, but ask yourself how many expert technicians and analysts that business model can support? And how quickly can they respond to a new threat on those resources? Lower cost software often has similar constraints – incurring soft costs such as support and resource drain. And everyone’s got a story relating how the most expensive option wasn’t necessarily the best value. Even high-profile commercial providers vary in the resources they invest in research, development, and customer support – regardless of how high their prices are.

From overall expenditures to ease of management and quality of protection, it’s clear that the total cost of protection is too high for many organizations.

For information about Kaspersky Lab’s commitment to providing security solutions that provide you with the best Total Cost of Protection, click here.
About Kaspersky Lab

Kaspersky Lab is the world’s largest privately held vendor of endpoint protection solutions. The company is ranked among the world’s top four vendors of security solutions for endpoint users*. Throughout its more than 16-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. With its holding company registered in the United Kingdom, Kaspersky Lab operates in almost 200 countries and territories worldwide, providing protection for over 300 million users worldwide.

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

www.kaspersky.com/business

SEE IT. CONTROL IT. PROTECT IT.
With Kaspersky, now you can.


© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners.