CYBER SECURITY FOR BUSINESS – COUNTING THE COSTS, FINDING THE VALUE

Business has always looked to squeeze the maximum possible benefit out of IT resources at the lowest possible cost – but measuring return on investment isn't so easy.

EXECUTIVE SUMMARY

When a breach occurs, every second counts – and costs. But few companies have a handle on the ROI for their cybersecurity efforts. How can you find the value? What if weighing up the different payoffs could help your organization focus on the cyber security solutions that best fit – and, in the process, derive the best possible bang for their buck?

The cyber security solution you implement impacts ROI:

Classic/traditional: mostly on-premises, supported by large admin teams in larger businesses.

Cloud solution: managed via cloud-based console and tools, with no additional hardware.

Outsourced: where an external third party service provider – a "Managed Service Provider" (MSP) takes care of everything.

Each brings its own benefits and budgetary impacts but for companies with limited in-house resources – or that prefer to outsource to a third party for management – cloud-based cybersecurity represents the best value, form both an ease of management and cost-efficiency perspective.

WHEN LESS HAS TO DELIVER MORE

“Do more with less” has become a business mantra over the past few years, but it’s nothing new to IT professionals. Business has always looked to squeeze the maximum possible benefit out of IT resources at the lowest possible cost – the real challenge for IT pros today is keeping pace with complexity in the face of limited resources.

And when it comes to cyber security, businesses of all sizes are struggling to keep up with constantly evolving threats while maintaining control over an ever-expanding range of hardware, devices, applications and end-users.

Back in 2013, PriceWaterhouseCooper reported a decline in hiring cyber security staff; at the time, Kaspersky Lab research found 58% of companies admitting their IT security was under-resourced in at least one area of staff, systems or knowledge. Fast forward to Q4 2016, and businesses are talking about a cyber skills shortage – and expanding their budgets to meet it.

But this isn’t just a skills story: 40% of companies today point to increased infrastructure complexity as a key driver of cyber security budgets. Interestingly, no one seems to have a handle on what the return on investment for their cybersecurity efforts is: 62% of large companies and 59% of SMBs says they’ll continue to invest regardless of their ability to measure return.

So how can companies break down the return on cyber security investment? What if weighing up the different payoffs could help your organization focus on the cyber security solutions that best fit – and, in the process, derive the best possible bang for their buck?

THE NUTS AND BOLTS OF CYBER SECURITY

Managing cyber security costs – and finding the returns on investment - ultimately breaks down to three key, intertwined areas: CAPEX, OPEX and Human Resources. In plain speech, that's how much kit you need, how much it's going to cost you to manage it and where you're going to find the people to oversee both.

LET'S START WITH CAPEX:

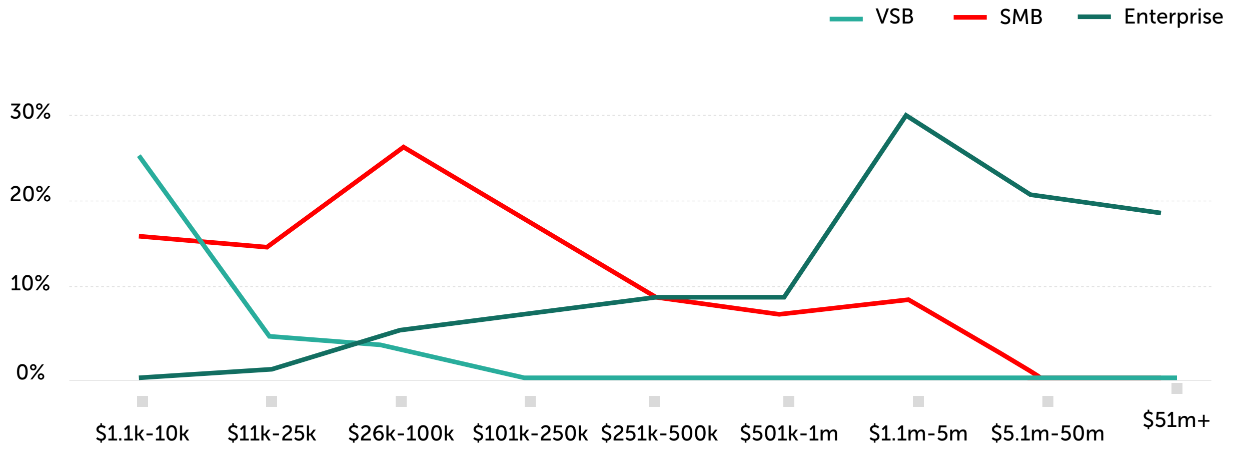
If you're a CISO or cyber security manager, you'll be pleased to know that budgets are increasing, with the approval of senior management: 38% of large businesses and 33% of SMBs say top management is asking them to ramp up cyber security investment.

The other side of this coin, of course, is that expectations in terms of what can be delivered are higher. One downside of increased cyber security investment can be complexity – more hardware, more devices, more applications – all needing to be integrated, managed, monitored. It's a fact that, for every 25 per cent increase in functionality, there's a 100 per cent increase in complexity. Fifty-five per cent of SMBs point to the growing volume of devices they need to secure as a key challenge.

Who's going to manage all this stuff?

That brings us to OPEX and HR – both essentially about skills...

IT Security Budget



Percentages of businesses whose IT security budget lies in each range.

THE HUMAN FACTOR – COUNTING THE COST OF A CYBERSECURITY SKILLS SHORTAGE

Despite more than half (54%) of SMBs believing their IT security will be compromised at some point – and understanding that preparation plays a critical role in prevention and detection – 40% say they lack sufficient insight or intelligence on the threats faced by their business.

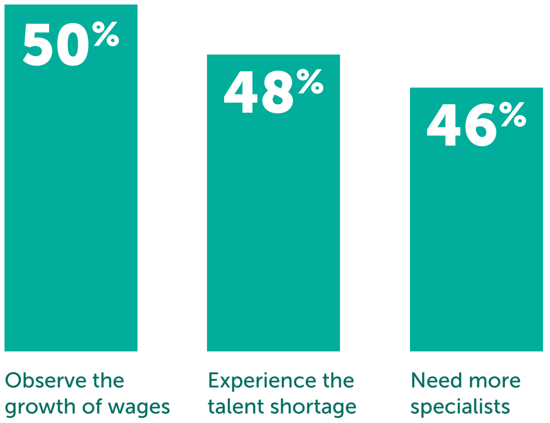
When you consider that the average SMB's IT team of 16 has only two security experts , it's easy to understand why human resources are playing at least as important a role in cyber security planning as any technology or infrastructure concerns. No wonder more than a third of businesses worldwide see improving specialist security expertise as one of the top three drivers of cyber security investment, with half saying there's a talent shortage.

The most worrying thing of all? Research shows a clear line between availability of talent and the cost of recovering from a breach: enterprises struggling to find the best security talent spend an average three times more recovering from a breach; a significant amount of recovery costs for SMBs comes in the form of increased staff wages (an average $14k).

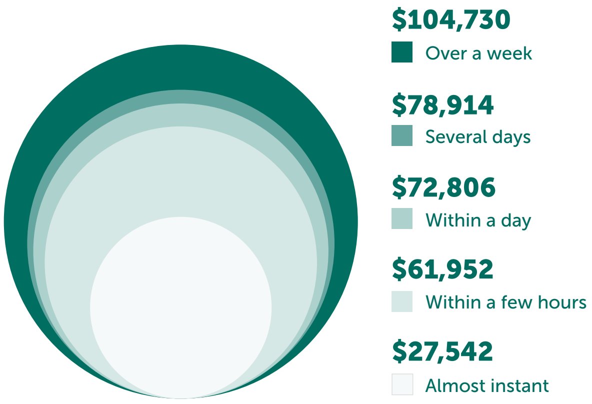
The adage that 'time is money' could have been written for cyber security; when a breach occurs, every second counts – and costs. A breach detected almost instantly costs the average SMB $28k, rising to $105k if undetected for more than a week. In actual data terms, an average of 417 records are compromised, even with instant detection. This rises to more than 70,000 when undetected for over a week.

Bottom line: Human resources are as important as technology resources in fighting cyber threats. It's how you find the right balance for your business that counts.

The human factor



Time is money



HORSES FOR COURSES: HOW THE CYBER SECURITY SOLUTION YOU IMPLEMENT IMPACTS ROI

Business cyber security comes in three main flavours:

Classic/traditional
Mostly on-premises, supported by large admin teams in larger businesses.

Cloud solution
Managed via cloud-based console and tools, with no additional hardware.

Outsourced
Where an external third party service provider – a "Managed Service Provider" (MSP) takes care of everything.

Each brings its own benefits and budgetary impacts.

TRADITIONAL, ON PREMISE SECURITY:

The classic approach is the original do-it-yourself cyber security program. In-house teams of technology, financial and business decision makers choose the solution (or solutions) that best fits company needs, including the hardware resources to support it, and manage everything in-house themselves. On the plus side, having everything in house gives maximum control over security – the down side is that you need to have the in-house skills and resources to exploit that benefit.

Companies that opt to use different vendors for different components of their security also introduce the twin problems of complexity and integration – again, areas that place additional demands on in-house skills. Organizations that use traditional cyber security approaches can reduce costs by opting for solutions that offer centralized consoles, enhanced systems management and automation capabilities and the ability to secure and control disparate devices. You'll be reducing time spent on day-to-day tasks for admin staff – but ultimately still need to ensure you have the required skills in place to keep everything running properly.

Approximate costs for a company with two offices and 100 endpoints in total

TYPICAL COSTS ($)*	ANNUAL COSTS ($)
Offices connected via a network	
Admin resources for IT security: $,4000 a month	48,000
Hardware: at least $3,000	one-off costs
Cybersecurity software: €4,614(around $4,800) for a one-year license	4,800
In-house skills training: $1,500 a year	1,500
TOTAL ANNUAL COSTS	**54,300**
TOTAL ONE-OFF COSTS	**3,000**

**Costs are approximate and for information only. Costs for specific business situations may vary from these.*

CLOUD BASED SECURITY:

With almost two thirds of SMBs already using an average of three cloud solutions, it's not surprising that Cloud-based security is one of the fastest-growing options available. The low cost of entry, ease of management and flexible licensing options are well suited to SMBs looking to scale on demand – in any direction.

What makes cloud-based security particularly appealing on the budget front is that it's very quick to rollout, even easier to manage and requires no additional hardware investment. Because all the necessary infrastructure is hosted by the vendor in the cloud, there's no need for customers to buy or maintain a server (or a license for it) for their management console. This allows smaller businesses to use leading-edge security solutions without having to hire additional skilled staff or high-end hardware to manage it. For SMBs struggling to grow the expertise to protect themselves from increasingly sophisticated threats, this is a real win-win scenario.

A key reason for this is that the cloud-based console enables the management of multiple endpoints, mobile devices and file servers remotely, from anywhere. They're usually ready to run and highly intuitive – meaning IT admins without specialized security skills can easily use high-end security features. Default security policies developed by skilled cyber security analysts bring ready-made intelligence and best practices in-house – without having to make new hires or train existing employees to use the new cloud console. Everything's intuitive and ready to run.

Because everything is centralized, administrators of cloud-based security solutions can monitor the security status of up to 1000 corporate network nodes from any chosen online device, from any location. Reporting and license tracking are easily managed via a simple, intuitive interface. You get the best security – while getting the best out of your current staff.

TYPICAL COSTS ($)*	ANNUAL COSTS ($)
Approximate costs for a company with two offices and 100 endpoints in total	
No need to connect offices via network	
Admin resources: $2,000 a month	**24,000**
License fee: €200 (around $208) a month	**2,500**
Basic in-house skills required: $7,000 a year	**7,000**
TOTAL ANNUAL COSTS	**33,500**
TOTAL ONE-OFF COSTS	**0**

**Costs are approximate and for information only. Costs for specific business situations may vary from these.*

OUTSOURCING TO A MANAGED SECURITY SERVICE PROVIDER

This option takes cloud-based security a little further – instead of someone in-house operating the cloud-based controls, a business can outsource management to an expert third party that doesn't need to be on-site to be in control. You get all the advantages of a leading security solution without putting a strain on budgets. No wonder 40% of SMBs and 26% of very small businesses say they think MSPs could be the answer to their security needs. Almost a quarter of SMBs plan on adopting this approach to security in the next 12 months.

The real benefit of outsourcing to an MSP for security is that businesses of any size gain access to the best security talent without having to invest in it or gain expertize to manage it themselves. SMBs could implement enterprise-grade options without needing a budget to match. And because the MSP has the in-house expertise, you can save on paying for up-to-the-minute security and threat intelligence – and trying to interpret it. As with cloud-based solutions, the MSP option has a great element of flexibility – because the software vendor is running the infrastructure, it's usually very easy for the MSP to accommodate seasonal flexibility or other scaling requirements. This can save a lot of headaches with licensing and subscription budgeting and management.

TYPICAL COSTS ($)*	ANNUAL COSTS ($)
Approximate costs for a company with two offices and 100 endpoints in total	
No need to connect offices via network, but should be within reasonable distance of MSP partner.	
All IT: $3,000 a month	**36,000**
No in-house skills required	**0**
TOTAL ANNUAL COSTS	**36,000**
TOTAL ONE-OFF COSTS	**0**

**Costs are approximate and for information only. Costs for specific business situations may vary from these.*

THINK DIFFERENTLY, MAXIMIZE VALUE

Complexity undermines security, efficiency and growth. It creates room for error and limits your ability to manage change. IT professionals are all too aware of the challenges. But what can you do to mitigate them without restricting end user needs or over-burdening already strained resources?

By exploring cyber security options you may not have previously considered – such as cloud-based or MSP, you could enhance the return on investment you get from security. Free up IT admin time and reduce the need for in-house expertise or new hardware with cloud-based or outsourced security. Or stay traditional with an on-premise solution – but one that offers centralized controls and the kind of advanced systems management features that help you get the best out of human and infrastructure resources.

Being prepared before something goes wrong has always been the best plan – if you can't find or can't afford additional talent, maximising the ability of existing staff by taking the complexity out of their jobs is a good idea. If you can't do that – why not outsource altogether? It all depends on where you're looking to maximize value. But thanks to the choices offered by Kaspersky Lab, when it comes to effective cyber security, your company doesn't have to run just to stand still.

READY TO CHOOSE YOUR CYBERSECURITY WEAPON?

If you've got a handle on the cybersecurity approach that best suits your business, it's time to put the theory to the test...

Are you an on-premise cybersecurity business? Download your free trial of Kaspersky Endpoint Security for Business and find out how powerful, intuitive controls, encryption and advanced systems management features can protect your business from even the most advanced threats.

Headed for the ease of use of the cloud? Sign up for your free trial of Kaspersky Endpoint Security Cloud <here> and see for yourself how you can reduce costs and resource overheads by managing multiple endpoints, devices and file servers remotely, from anywhere.

Outsourcing to a third-party expert? Visit Kaspersky Lab's Managed Service Providers page.

Kaspersky Lab global Website

Kaspersky Lab B2B Blog