Tipping Point: Why Enterprise Security Must Change

10 Top Takeaways

In today's digital world, data is the currency giving businesses the power to act decisively and swiftly, provide rich customer experiences and remain one step ahead of the competition. But, as data becomes more valuable, it also becomes more vulnerable.

Organisations are running their critical operations on emerging digital technologies, deploying more applications on more devices in more geographies than ever before. However, this digital approach is also creating greater exposure to equally sophisticated levels of cyber attacks, meaning a much higher level of protection is required to protect business critical data.

Security spending has grown over the past few years – reaching $75.5bn in 2015[1] – but the cost of breaches is also increasing as risk levels continue to rise.

Worryingly, IT teams are holding back details of some of the most serious cyber security breaches, leaving business leaders in the dark as to the true extent of the issue. These fractured lines of communication, combined with the increasing complexity of a digital-first approach to business, has led to a disconnect over security planning and priorities.

To better understand this disconnect, we gathered insights from 1,700 IT decision makers (ITDMs) and 3,500 office workers from across EMEA. Here are our top 10 takeaways:

1 Bring security to the top of the boardroom agenda

Despite the fact that organisations are under increasing threat of serious cyber attacks – with more than a third (37%) of ITDMs expecting to be hit in the next 90 days – corporate leaders are not prioritising cyber security. To put that in context, less than one in ten business leaders in EMEA[2] (8%) consider it a priority for their business.

A reason senior management have not prioritised cyber security is they simply don't know the extent of the problem. As demonstrated in our research, a quarter of ITDMs (25%) admit they have, on at least one occasion, failed to disclose a significant data breach to senior managers.

More must be done to ensure that business leaders and IT are having the right conversations around security planning and priorities, and ensuring that the topic is a key boardroom talking point.

[1] Gartner – Forecast Analysis: Information Security, Worldwide, 2Q15 Update

[2] Research from Economist Intelligence Unit – 1,100 senior executives, recruited from companies between $500 million and $5 billion in revenues, on data security practices within their firms.

Protecting critical business assets, including IP, business plans, customer data and financial results, that a company's performance and reputation rests on, needs to be an ongoing discussion point for business and IT leaders. Traditional models of security that reinforce the perimeter are no longer working and so a new model is required – one that protects a company's crown jewels. A software-enabled architecture can do this: building security into everything and providing the speed and ability to enable organisations to immediately respond to emerging threats and attacks.

2 Security needs to be a business-wide priority

Unfortunately, ITDMs and office workers are failing to put enough focus on data security. The former places cost cutting at the top of their agenda (45%), while the latter names acquiring new customers (51%) as their most important aim.

Whilst cost cutting will continue to remain important as IT budgets remain fairly flat, security needs to become a greater priority across the whole of the business, from the IT department, right through to business leaders and employees. That means making sure staff know what's expected of them when it comes to meeting security processes as well as educating on the pitfalls of not being compliant.

3 Accountability must rest with the Board but responsibility extends to IT and employees

Whilst the whole business should treat security as a priority, our research showed that almost a third (30%) of ITDMs and almost a quarter (23%) of office workers in EMEA believe the CEO should be held accountable.

A business' worth and reputation rests on its ability to safeguard valuable data, such as its IP and business plans, and as such the Board is accountable. IT leaders must adopt ways to ensure this is protected. But everyone within the business has a role to play, from the employees' responsible use of their mobile phones and apps, through to the Board truly understanding the security threat landscape, having visibility of threats and the technology choices for mitigating them.

4 Protect while enabling mobility

Many organisations feel the greatest security vulnerabilities come from inside the business. Nearly half of ITDMs (45%) cited employees who are careless with company data or untrained in cyber security processes as a key worry.

Additionally, more than a fifth (22%) of employees said they are happy to risk being in breach of their organisation's security policies to carry out their job effectively.

When done the right way, IT departments can enable the workforce to work productively while remaining secure, offering them a choice of devices with the supporting tools needed to do their jobs. Consumer-simple, enterprise-secure mobility solutions mean that organisations can give employees access to the apps and information they need, in the way they need it, while being able to manage, access and enforce security. Taking an end-to-end approach to security, protecting information and apps from the end-user to the desktop to the data centre, whether on premise or in the cloud-as-a-service, is the key.

5 Security breaches can have a wider impact than initially thought

In addition to the business damages of reduced customer trust, loss of confidential data, and impact of future revenue, our research found that staff morale was also likely to be squashed in the wake of a security breach. In fact, 45% of ITDMs felt they would consider leaving their organisation if the company suffered a significant data breach.

Businesses need to have a contingency strategy in place ensuring that, should a data breach occur, it is quickly contained, efficiently controlled and effectively communicated, to minimise impact.

It is more cost-effective to invest in the right security strategy than it is in retention of customers and employees, not to mention the financial damage caused by loss of reputation.

6 Make employees aware it will directly impact them

Today's tech-savvy employees do have a level of understanding of the value of data. A third (33%) take greater care of securing data on their personal device than looking after the information on their corporate one. Indeed, 33% are more concerned about losing personal data than corporate data.

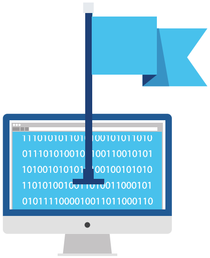
Employees need to understand the consequences of a workplace security breach. After all, an incident that damages the reputation of the company can have financial ramifications, possibly even impacting their own job security. Help them to understand the real and often personal cost of security breaches, and you can be sure that the workforce will quickly change their ways.

7 Driving compliance across the business – no exception

While it is important the IT department offers workers the tools and services they need to remain at the forefront of their industry, everyone across the whole company needs to understand there can be no exceptions when it comes to security policies. Worryingly, 66% of ITDMs admitted they'd felt under pressure from the senior leadership team (36%), C-level executives (35%) and department heads (28%) to circumvent the rules.

Everyone, even the most senior leaders, needs to understand that some security rules go beyond the company itself, and breaking your organisation's security policy – even if you are the CEO – could have compliance ramifications. All parties must therefore have a strong understanding of the pressures and limitations each other faces. This means regular contact, and close collaboration across departments.

8 IT needs to take the reins



With serious concerns over the safety and security of an organisation's data, it is vital someone steps forward to take control. The IT department is the obvious candidate – with 77% of ITDMs believing they are in the best position to do so.

And with more than three quarters (76%) of office workers putting their faith in IT to protect against cyber attacks, all eyes are on the department to take the reins in the race for data security.

Using VMware's One Cloud, Any Application, Any Device™ architecture, organisations can create the foundation for a secure framework which allows the freedom employees demand, with the reliability and security needed to operate safely when faced with external threats. A network virtualization platform offers the opportunity to not only transform every aspect of how security should be addressed, but has created a security layer where all security innovations are more manageable – enabling IT to constantly keep up with the latest threats.

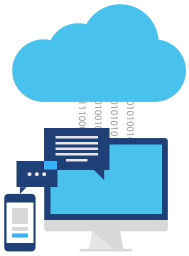
9 Agile security from the inside out

With the complexities of increasingly digital businesses, current security methods are struggling to simply keep pace. In fact, more than a third (35%) of ITDMs in EMEA believe their greatest vulnerability is cyber threats moving faster than their defences.

With applications and user data on more devices and locations than ever before, old security models that focus on reinforcing the perimeter are no longer working. Organisations must move beyond the traditional approach to IT security. Security must be built in the core of the infrastructure from the data centre to the device, automatically protecting even against unknown threats. They need an architecture that fortifies security from the inside out – inside the application, inside the network, and at the user and content level.

Only a software-defined architecture for security can deliver the speed, agility and automation that businesses need today.

10 Virtualize for a fresh approach



Of course, if the IT department needs to take control, they must have the right technologies to support them. A number of organisations across EMEA are recognising the value of virtualizing at the server, network and storage levels to create the foundation for a comprehensive architecture that enables security to be built into the technology infrastructure. There are a number of smart organisations already doing this:

For the University of York in the UK, protecting its Intellectual Property is key and network virtualization is at the heart of the security strategy. With network virtualization, academics can rapidly access secure servers for their research, and IT can control user access to data and applications on the network. The university moved away from the inadequate perimeter approach to security, to one that starts with security from the inside. Network virtualization is helping The University of York safeguard its IP, its students and its reputation.

Meanwhile, the third largest private charity donor in the world, Novamedia, needed a highly-secure IT platform to support rapidly growing revenues and a wealth of financial data relating to donations. It has virtualized the network to secure the environment, so every virtual machine (VM) is firewalled, isolated, and segmented, to secure the data centre from hackers. With more robust security in place, the billions of Euros it handles each year are better protected.

King Abdulaziz City for Science & Technology's (KACST), Internet Services Unit (ISU) provides Internet and IT services to the education and government sector in Saudi Arabia. Using VMware NSX and VMware vRealize Automation, ISU is providing its customers with cloud services which have automated security controls inside the data centre.

In Summary

- Any organisation's success depends on its ability to provide the best customer experience, to respond swiftly to opportunities and to safeguard its brand and customer trust. Data is at the heart of this strategy; its importance, and its vulnerability, cannot be overestimated.

- The era of the digital business and sophisticated threats demand a new approach to brand protection and earning customer trust. Old security models – both the technologies and the processes – are just not working. And as the number and the sophistication of threats grow exponentially, they now have the power to put organisations out of business.

- The disconnect between business leaders and IT decision makers over security planning and priorities, combined with the complexity of having to manage more business applications and data on more devices in more locations, is forcing this rethink of security. The CEO will focus on reputation and risk management while IT is focused on defending IT assets. One of the changes IT leaders need to embrace is having clear discussions around the vulnerability of certain IT assets and the reputational risk of those assets being compromised.

- What is required is a software-defined architecture for security, built into the fabric of the technology infrastructure from the data centre to the device. Virtualization offers a platform for this new architecture, allowing organisations to fortify security from the inside out – inside the application, inside the network, and at the user and content level.

About VMware

VMware (NYSE: VMW), a global leader in cloud infrastructure and business mobility, accelerates our customers' digital transformation journey by enabling enterprises to master a software-defined approach to business and IT. With VMware's One Cloud, Any Application, Any Device™ architecture for IT, organizations are creating exceptional experiences by mobilizing everything; differentiating and responding faster to opportunities with modern apps hosted across hybrid clouds; and safeguarding brand and customer trust with a defence-in-depth approach to cybersecurity. With 2015 revenues of $6.6 billion, VMware has more than 500,000 customers and 75,000 partners worldwide. Learn more at vmware.com

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com