

Bringing up baby

Sold for so long on the basis of fear, uncertainty, and doubt, has the time come for IT security to grow up and start delivering more bang for its end users' buck?

For a technology whose purpose seems, on the face of things, so apparently clear cut and straightforward, IT security is on many levels, a bit of a paradox.

On one hand it's a subject about which any number of companies claim to be an authority. On another it's been known to leave even the most expert expert completely exasperated. Here too, while 'security' is often as far removed as it is possible to be from a business's perceived core activities, it's also something that anyone who runs one now has to consider on virtually a daily basis. Go figure.

Most ironic of all however, is the fact that many organisations still see IT security – a discipline specifically designed to protect and safeguard them – not as a saviour, but as a necessary evil. And one that's getting more and more necessary by the day.

Time was when we only needed to protect our servers and LANs. Then it was our desktops, our laptops, and our palmtops. Then came the VLAN, the WAN, the WLAN and the myriad of flavours, hybrids, and variations thereof. Network security suddenly had to think bigger, and stretch beyond the business's traditional and physical boundaries.

And now – with the emergence and growing influence of terms like disaster recovery (DR), business continuity (BC), compliance, and corporate governance – it looks as though things are moving on once again. Because with an ever-burgeoning raft of associated legislation to contend with, enterprises no longer have a choice when it comes to maintaining truly robust defences. They **have** to.





The long and the short of it?

Security technologies are now under pressure to transcend traditional ideas of 'security'; to do more than simply 'secure'.

Indeed, New York-based consultancy TheInfoPro's recent survey of 147 Fortune 1,000 IT managers found that over 70% were increasing their budgets to meet requirements like Sarbanes-Oxley, Basel II, and the Payment Card Industry (PCI) data security standard.

So what should businesses expect from their security investments these days? What can they expect?

And what does this mean for the enterprise in terms of agility? Cost? Competitive edge?

"Ultimately, the aim of any technology is to help your organisation be more competitive", says Paul Irvine, Sales and Marketing Director at Bloxx.

He believes with legal threats and compliance requirements growing in direct response to world changes, the pressure and demands on those responsible for protecting any organisation must be at least commensurate with that.

Accordingly, he says, security now has to be seen in a business context. That's about much more than keeping your data safe from theft or loss; staff productivity has to be protected too, as does the overall smooth running of the business.

"Since my first days in IT, I have used the phrase 'it pays to be paranoid'", says Irvine of how to approach this challenge, adding that such an attitude has "saved his skin on a number of occasions" and that it's more applicable today than ever.

But with so much to consider and a plethora of consultants and solutions to choose from, where should enterprises search for that extra yard of performance and value for money?

Ed Farquhar, VP of Marketing EMEA at ArcSight, suggests that companies should first look carefully at themselves, consider their ability to monitor, respond, and adapt to potential threats and IT management and governance issues, and to do this from the top down. "Security, compliance, and governance are now hot topics for board members, not only over-worked security and network operations centres", he says.

You can't have security without implementing a DR strategy

Andy Kellett, research analyst at the Butler Group, says that market changeability must also be a major consideration. "It is not just the range of threat models that constantly changes", he says. "New product developments, new network infrastructures, new acquisitions, the constant availability of new technology tools. All continually contribute to an organisation's constantly changing risk profile."

Kellett asserts that after a period of using piecemeal, fragmented systems, companies are reaching out towards security solutions rather than point-based products, and to vendors that take responsibility rather than running for cover at the first sign of trouble.

This is particularly important at a time where data volumes are exploding

and timescales for data recovery and restoration are plummeting. It involves keeping your eye firmly on the ball; the problem for most enterprises tending to be that they just don't know what they have sitting on their networks.

"Companies need to have long-term strategies for dealing with this; not only data retention policies, but appropriate technical infrastructures to enable them to respond effectively to disruptions wherever and whatever they are", explains Ron Miller, managing consultant at SunGard Availability Services.

This demands taking a fresh look at existing security and DR strategies and trying to view them as a whole or, as Miller puts it, looking at security and DR in tandem.

"You can't have one without the other... it's not just about DR, which implies failure and then recovery. It's much more about continuity in the 'always-on' environment in which many companies operate."

Predictably, such operational nirvana is easier said than reached. It is though, achievable with the right planning, the right solutions, and the right support. Unfortunately, according to Farquhar, some vendors are still employing 'smoke and mirror' tactics to disguise weaknesses in their offerings, which doesn't help.

He suggests evaluating pure-play, specialist vendors as opposed to generic IT companies looking to "take a ride on market demand."

Here, says Geoff Webb, Security Product Manager at FutureSoft, the true measure of a security technology's ROI is not just the



It's a far cry from a security landscape that just a few years ago, saw distributed systems security as more or less an anti-virus issue. These days the focus of attacks has switched to stealing data, ID theft, and holding companies to ransom...



degree to which it addresses vulnerabilities, but also how much it enables business processes.

He reasons that good security should provide protection within a framework of sound operational efficiency. i.e. implementing appropriate security policies and processes can enable the business to more fully understand its own operational processes and to get a better grasp on its assets.

"There is most definitely a strong trend towards convergence between security and business (which will) continue to provide cost benefits as well as enhanced security", he adds.

It's a far cry from a security landscape that just a few years ago, saw distributed systems security as more or less an anti-virus issue. These days the focus of attacks has switched to stealing data, ID theft, and holding companies to ransom, according to Simon Perry, VP of security management at CA. "There is also more of an awareness of the internal threat from rogue or simply ignorant users."

This change has led to at least two strategic shifts in the marketplace, says Perry.

First of all, he explains, the smaller 'pure-play' vendors like Witness Systems, Sophos, F-Secure, Trend Micro, and McAfee have acknowledged that security is not just about things like anti-virus with a 'dash' of firewall. (*"Some would say that they are trying to outrun the Microsoft train that they sense is approaching them."*)

At the same time, the major software houses are including security amongst a broader set of offerings. "I would include CA in this category as you might expect, but also IBM, Oracle and the like."

"We feel that security cannot be addressed as a stand-alone issue. Where does the line between disaster recovery, business continuity, and security management lie? The answer is that they are interwoven."

Perry doesn't think the market has yet reached a point where it has switched from pure ROI to value on investment (VOI) however. So in terms of businesses getting 'peace-time' enablement value from their security strategies, his message is clear: "Simply put, without security you cannot use the Internet for

commerce. (And) you cannot use the Internet for customer loyalty programs. And while you're at it, you may as well shut down the use of email and collaboration tools."

This is because transactional Internet usage requires user authentication; something he says is "fundamental", especially as consumers become hyper-sensitised to security issues.

Perry thinks that, within five years, customer choice will be swung by factors such as trustworthiness as they seek reassurances about the use of their data. "Price, features, brand loyalty... all these factors will still be in play, but 'Do I trust them with my data?' will come into the mix too."

What of the central question then? "Should I expect more from my security investments?"

The answer is yes. With one caveat.

Security can only operate outside the box if the business learns to think that way.

Security for
the future

ZyXEL