Research

Bloor

The Ongoing Security Paradox

The third Global Study quantifying the cost of Reactive versus Proactive security in a mid-sized organization

A Research Paper by Bloor Research
Author : Nigel Stanley
Publish date : September 2010

Threats come in all shapes and sizes, but all of them can, ultimately, cause damage to an organization

Nigel Stanley

Foreword

Cybercriminals, hackers and malware. Just a few of the threats that mid-sized organizations across the world now worry about. As well as being a huge distraction from their day-to-day business these threats can have a real, tangible and detrimental effect on a company. The scale, diversity and volume of these threats increases each year—in 2009, for example, McAfee® Labs rated more than 27 million domains and found nearly 6% of them to be a risk, compared to 4% of the 9.9 million websites that were analyzed in 2008 (source: McAfee Security Journal 2010). This explosion in risk creates even more pressure for mid-sized organizations that are struggling to grow their businesses against a background of competitive pressures and very slow recovery from worldwide financial turmoil.

This is the paradox for IT generalists in mid-sized organizations: enable the business to grow across new channels and create new ways to get business done whilst, at the same time, protect corporate assets and information with limited resources and budget. Threats up, budgets down—the "security paradox", as it was named in last year's report.

Not all the threats come from outside an organization. In many instances it is previously trusted employees that steal customer information, financial data or product plans. Privileged access to internal data, coupled with a disenchanted member of staff, is a recipe for disaster and a tough problem to address. In the past attempts were often taken to suppress such wrongdoing, however, legislation and compliance oversight, coupled with social networking, requires these events be reported for all to see. Reputational damage is now a big issue.

This year, as last year, this report examines the security spending of mid-sized organizations (51–1,000 employees). It is recognized that the structure and capability of an organization with 51 people is radically different to that of one employing 1,000 people but the key issue they face is the same—addressing IT security threats as cost effectively as possible.

These threats are a reality. 83% said they were concerned or very concerned that their business could be the target of an intentional and malicious security attack. 51% had actually been attacked, 16% of which took over a week to recover. For an unfortunate 4% this recovery took a number of months, a significant distraction from running a mid-sized business. Data loss was the number one consequence of the attack.

It's not all bad news.

IT security vendors continue to work hard to produce solutions to reduce the risk of damage to an organization from cybercrime and hackers. By putting in place a well thought out and managed IT security solution, companies can significantly reduce their chances of suffering from an attack. This will enable the business to focus on its key objectives, such as developing new business areas during this critical financial recovery period.

Methodology

This survey was conducted by Bloor Research on behalf of McAfee. In excess of 1100 surveys were completed with respondents having the following criteria:

- Employed in a company with 51 to 1,000 employees worldwide
- Responsible for IT purchasing, management or have overall ownership for governance, risk and compliance within their organization
- Employed in the private sector (i.e. excluding government, education and non-profit organizations).

The survey was conducted on both the telephone and the web and covered the following countries:

Australia	Brazil	Canada
China	France	Germany
India	Japan	Mexico
Netherlands	New Zealand	Spain
UK	USA	

Data was also aggregated into geographic areas for analysis:

- Asia Pacific (APAC)
- Latin America (LTAM)
- Europe, Middle East and Africa (EMEA)

Key findings worldwide

54% of mid-sized organizations have seen an increase in IT security risks facing their company from 2009 to 2010, up 2% on last year.

40% of mid-sized organizations have had data breaches in the past year, an increase of 13% from last year.

75% of mid-sized organizations said that there is a chance that a serious data breach could force them out of business, up from 70% in last year's survey.

30% of mid-sized organizations had to manage multiple network security incidents, of which 55% took up to 5 hours to investigate and remediate.

58% of worldwide respondents spend less than 3 hours per week working on, evaluating and researching IT security. Last year it was 65%.

5% of mid-sized organizations reported that they had suffered a data loss that had cost them more than $25,000. Of these 25% were from China, 14% from France and 11% from India.

47% of all reported intellectual property losses were from EMEA-based mid-sized organizations.

88% of mid-sized organizations said they were concerned or very concerned about non-malicious/inadvertent security incidents.

60% of worldwide mid-sized organizations admitted to knowing less than 75% of the pertinent regulatory and compliance requirements pertinent to their organization.

Analysis of threats, incidents and responses

Threats come in all shapes and sizes, but all of them can, ultimately, cause damage to an organization. Respondents were asked to quantify the number of incidents they had been subject to over the past three years, and whether these were unintentional/inadvertent (such as the accidental loss of a laptop) or malicious and intentional, such as a targeted hacking attempt. Interestingly, 53% had suffered between 1 and 5 unintentional incidents and 46% had suffered between 1 and 5 malicious attacks. It was encouraging to see that 17% of respondents had suffered neither, suggesting they had good protection mechanisms in place or good luck prevailed. More likely it was a combination of both.

The threat that most organizations had experienced was malware on PCs and laptops, which accounted for 16% of all incidents, closely followed by malicious code attached to email at 15%. Of those reporting in excess of 21 threats or more in the year, 41% were due to email threats—malicious code attached to e-mails yet again. Clearly, some organizations had failed to remedy an initial security breach and were then subject to multiple follow-up attacks.

Website threats (such as phishing attacks, hacking and Web 2.0 attacks) made up 12% of all threats seen by mid-sized organizations and 10% of all incidents that occurred resulted in the loss of data to the organization under attack.

The reporting of data leaks and breaches is now mandated by law in many jurisdictions. The threat of publicity and associated reputational risk will often force even the most reticent business to implement data protection measures. Couple this with significant fines that regulators can now impose for each data leak incident and it's no surprise that mid-sized organizations are learning that data losses are no longer affordable.

40% of respondents said they have had a data breach in the past year, 5% citing frequent or very frequent data loss incidents. This compares to a reported 29% of mid-sized organizations suffering a data breach in last year's survey. This increase is probably due to more targeted attacks being waged against specific corporate data and intellectual property. An entire industry has developed around the commerce of buying and selling corporate data. Interestingly, only 6% responded to say that they have had to report a data loss publicly in the past year, which may or may not indicate the regulations they are subject to.

Europe, Middle East and Africa (EMEA) and Asia-Pacific (APAC) based mid-sized organizations figured highly in the frequent data loss category—in some instances with 5 times as many incidents as similar sized organizations based in North America.

The data being lost does vary but the most frequently lost data is private information (such as employee data or customer data) with 26% saying they had lost this type, followed by 23% for intellectual property and 16% for business plans. 47% of all reported intellectual property losses were from EMEA-based mid-sized organizations compared to only 13% from North America (NA). 41% of private information losses were from EMEA organizations compared to 15% in North America and 21% for APAC. Last year, 40% of the data lost in a security breach was the private information of customers, employees, and partners.

Analysis of threats, incidents and responses

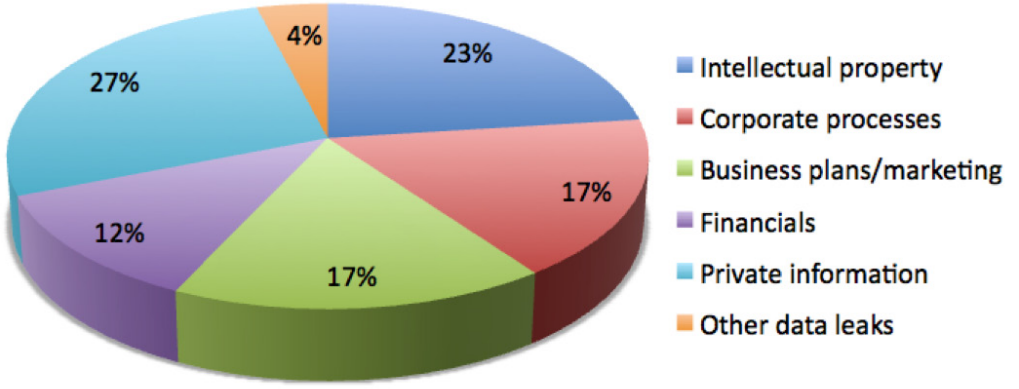

Figure 1: What type of data have you lost?

The cost of data breaches is important to any organization, and 5% of mid-sized organizations reported that they had suffered a data loss that had cost them more than 25,000 USD. Of these, 25% were from China, 14% from France and 11% from India. More importantly, 75% of mid-sized organizations said that there is a chance that a serious data breach could force them out of business. Last year it was 70%, so more organizations are thinking through the ramifications of a data loss incident.

Of those reporting up to 5 incidents, 30% were malware related, either directly on the end point or delivered via email. As email is now such a vital tool for business use it is easily exploited by cybercriminals intent on stealing data, especially as good social engineering can present an attachment in such a way that many users will open it.

Another recent development is the threats around cloud-based services. Cloud-based delivery of either IT infrastructure, software or services is gaining a lot of attention as they may offer reduced IT costs as processing is shipped to a third party. This should then enable a mid-sized organization to focus on their core business rather than running a large computing infrastructure. Inevitably, cybercriminals see this movement of data and processing as an opportunity to exploit insecurities and we would expect to see a growth in incidents in this area. Already 4% of respondents worldwide saw up to 10 cloud computing related incidents last year and 54% of these were mid-sized organizations from EMEA. Clearly, outsourcing a solution does not mean that the risk is outsourced as well.

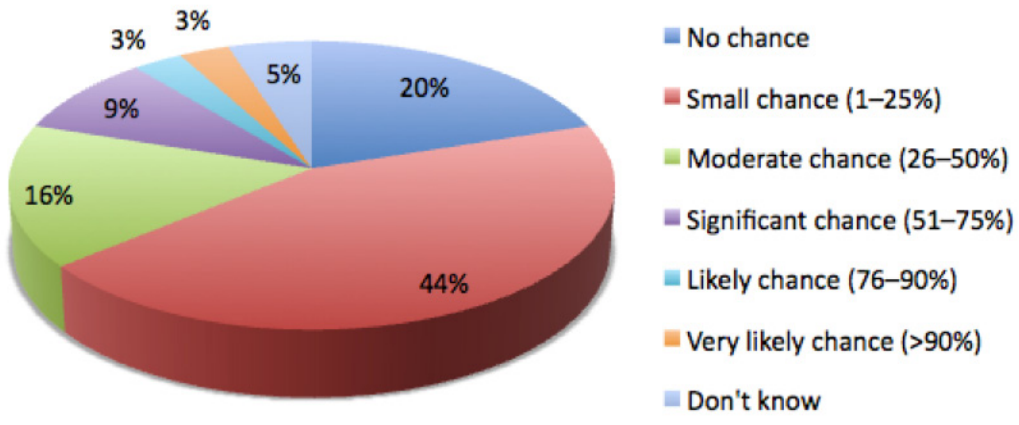

Figure 2: What is the likelihood for a company like yours that a serious data breach could cause that organization to go out of business?

Analysis of threats, incidents and responses

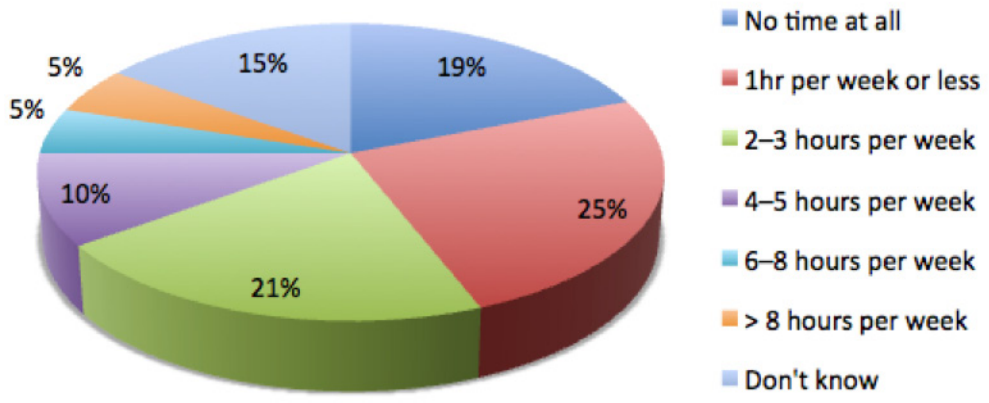

Figure 3: Approximately how long does each network incident take to investigate/remediate?

New areas for the report this year are emerging security threats within application code and mobile (cell) phones. Application code is frequently exploited by hackers looking to open a hole in a security infrastructure. Writing code so that all security flaws have been removed is very difficult, and as mid-sized organizations often purchase code and applications from third parties there is an increasing need to ensure the software is free from security bugs.

Mobile (cell) phones and smart phones have increasing amounts of processing power such that a smart phone today can match a desktop PC in terms of computing ability. The past year has seen an upsurge in hacker interest in compromising mobile (cell) phones and smart phones. These attacks often come in the form of Trojan software—innocent looking games downloaded from an application store that will siphon off e-mails, text messages and even bug voice calls—all unknown to a user. 4% reported up to 10 voice/content related breaches in the previous year, slightly more than had suffered cloud computing related incidents. Over the coming years this level of breach will inevitably increase.

The need for software patching is still with us. Vendors have dramatically improved their patch test and delivery cycle but the need to implement unscheduled patches is still with us. 46% of respondents worldwide have had to apply up to 3 unscheduled patches in the past year, on top of their routine patching release.

Networks are still vulnerable to attack due to their complexity and exposure to the internet. 39% of respondents worldwide had to manage up to 2 network security incidents, of which 55% took up to 5 hours per week to investigate and remediate. In many cases, this delay is due to the manual work involved in correlating network events and tracking down the cause.

Post-incident recovery time is crucial, so respondents were asked "Approximately how long did it take your company to recover from their most recent IT security incident/attack?" This included all the implications across the business, such as recovering systems and, importantly, the downtime of employees. 47% of worldwide respondents, lead by those in North America and EMEA, were able to recover within a day, and 35% within a few days. Naturally this depended on the type of incident as well as the systems, tools and mechanisms in place to manage such an event. For mid-sized organizations to be able to recover so quickly is a testament to their IT security skills. This can be contrasted against the 16% that took from a few days to months to recover—a very dangerous position for a mid-sized organization to find themselves in. Last year 37% reported that they have spent 3 or more days recovering from an IT security attack and 54% of UK companies recovered from an attack in less than a day. This year similar UK organizations are taking slightly longer to recover—only 49% claim to recover in under a day. Last year 40% of mid-sized companies in the United States took less than a day to recover from an attack, this year it is 54%, an encouraging increase.

The changing face of threats

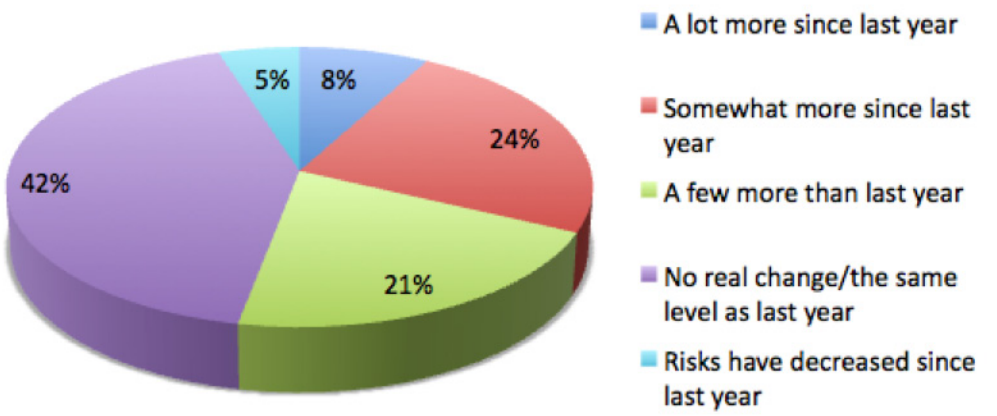

Figure 4: To what extent has there been a change of IT security risks (threats/incidents) at your company from 2009 to 2010?

Threats are undoubtedly changing on a day-by-day basis. Each morning brings news of a new vulnerability, flaw or aspect of IT that is now open to attack. Keeping on top of this is extremely difficult and, for mid-sized organizations working in industries away from computing, probably impossible. That said, and very importantly, 88% of mid-sized organizations said they were concerned or very concerned about non-malicious/inadvertent security incidents and 83% of worldwide respondents said they were concerned or very concerned about intentional security attacks. Interestingly, out of those reported to be very concerned, only 1% were from Japan, contrasting with 13% from EMEA and 9% from North America.

Clearly, mid-sized organizations get the message that their computer systems are vulnerable. This is borne out with 54% of worldwide respondents saying they have seen an increase in IT security risks facing their company from 2009 to 2010. This compares to 56% in last year's survey, a remarkably consistent finding. Of those seeing a lot more risks, 39% were from APAC. Of those seeing no real change 50% were from EMEA and of those that are seeing that risks have decreased since last year 35% are from the Latin America region (LTAM).

Attitudes are changing to IT security risks. 33% feel very protected from security attacks and threats but 7% feel not very or not at all protected. Of those feeling very protected 52% were from EMEA. 41% said they had never suffered an IT security attack but 51% said they had (8% didn't know). 13% of those that had suffered an IT security attack were from the United States. 7% of companies in the United States still don't know if they have been attacked; only 5% were in the same position last year but the year before that it was 15%, so these organizations are remaining reasonably aware, which is encouraging.

Asked about the size of organization most susceptible to attack and 16% chose the smaller sized—2 to 50 employees. Last year almost 50% of respondents said that organizations with more than 500 employees were most at risk from a security attack; that figure is now down to 21%.

This can be contrasted with the implementation of security technologies. 15% are happy to wait for an incident and then move quickly to remediate it, 35% are mandated due to regulations and/or customer requirements to be proactive and an interesting 10% do the minimum and hope nothing ever happens. Of those hoping nothing ever happens 26% are from EMEA and 27% are from APAC. Only 5% of Japanese mid-sized organizations have the same philosophy.

88% of respondents said that it was very or somewhat important for the IT security products they purchase to integrate with relevant technologies to enable the sharing of reports, intelligence and critical events. 27% said that they wanted their security products to leverage Directory Services and protocols, undoubtedly to make them easier to implement and use, and 23% said they wanted to leverage storage tools.

The changing face of threats

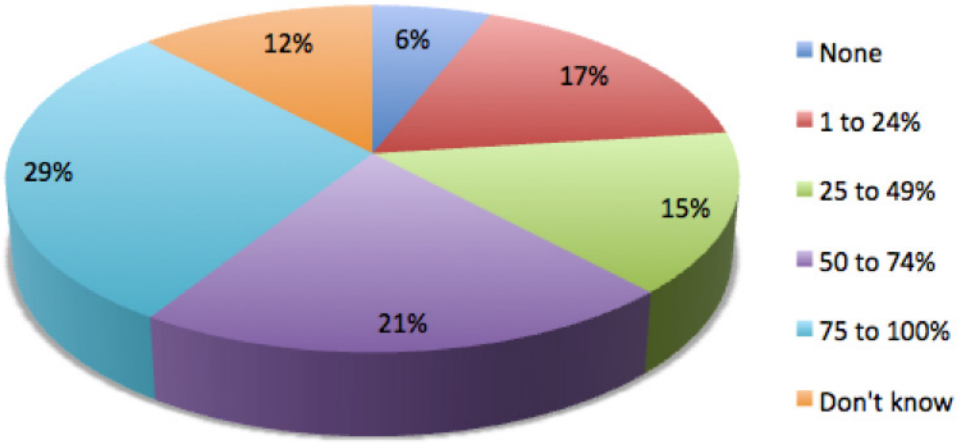

Figure 5: Please estimate what percentage of pertinent regulatory and compliance requirements are fully known and understood by your organization

IT security now seems to be an area of active interest and research. 58% of worldwide respondents reported that they spent less than 3 hours per week working on, evaluating and researching IT security. Last year this was 65%, so mid-sized organizations are investing a bit more time working on their IT security systems. 12% spent more than one day per week on similar research. Last year over 50% of mid-sized organizations in France spent less than 1 hour per week proactively working on security issues. This year it is 28%. Last year it was reported that 40% of mid-sized organizations in China spent less than 1 hour per week on proactive security, now that figure is down to 26%. US-based organizations spend more time on security related activities than any other country, a fact that remains consistent with last year's data.

29% responded that they had no staff working full time and dedicated to security issues but 51% reported that they had between 1 and 3 full time security staff. 95% of these were reported as being moderately or very competent, being able to manage almost all security incidents and situations.

Regulations form an ever-increasing backdrop to the information security posture of mid-sized businesses, and can hugely influence effort and expenditure. Understanding the amount of new and emerging rules, laws and regulations can be very difficult, so respondents were asked to estimate what percentage of pertinent regulatory and compliance requirements were fully known and understood by their organization.

A full 6% of worldwide respondents admitted to not knowing or understanding any of the pertinent regulatory and compliance requirements relevant their organization, and only 29% knew between 75% and 100% of those that apply. Of these, 31% were from North America and 33% from EMEA. Clearly this is an area in need of addressing to ensure that mid-sized organizations don't fall foul of the law. These regulations should also inform security expenditure, ensuring that tools and technologies that address these issues are prioritized.

This leads us neatly onto the general competency level of an organization's IT staff. Graded from very competent through to being challenged, the vast majority—95%—were deemed to be very or moderately competent. Only 4% were deemed to be challenged. This applied across all regions and countries in a fairly consistent way, although LTAM did dip comparatively in the very competent section. As respondents had to be working within an IT role maybe this question was not as objective as others in the survey!

The changing face of threats

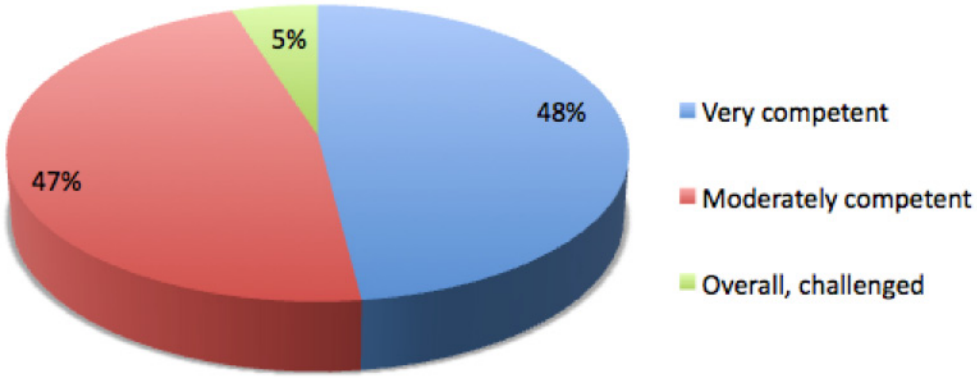

Figure 6: How would you describe the general level of competency of your organization's IT staff?

Costs and budgets

Budgets figure large in any organization today as costs are reduced against a backdrop of a poor economy. Inevitably, IT expenditure comes under the spotlight, quickly followed by IT security budgets. The majority of worldwide respondents, 62%, lump IT security and general IT budgets together, but 14% separate out security spend from the general IT spend. For many this may be a smarter way of accounting for security costs as they may be heavily influenced by compliance and regulatory needs across the business. This leads to broader thinking about information security and helps it receive budgetary attention in its own right. The range of security budgets is interesting. 30% have under $10,000 to spend annually but a lucky few—6%—have in excess of 100,000 USD for the year.

Despite economic pressures security budgets appear to fare reasonably well. 49% see the budget remaining the same as 2009, 20% see an increase for 2010 and 20% see a decrease for 2010. The results are very even across all countries, with no one country showing a particularly large increase or decrease. Last year, 75% of midsize organizations cut or froze their IT security budgets. Last year, more Indian companies increased their budgets than froze them; this year more Indian companies are keeping their budgets frozen rather than increasing or decreasing them.

For the IT security budget to remain the same or increase reflects a mature attitude towards IT security by mid-sized organizations as they see a need to continually push back against the rising tide of cyber threats to their businesses. Interestingly, in those that see a decrease in their budgets, 65% see a same level of protection despite the reduced spend. 8% said that a decrease in their budget will lead to more protection, which is interesting.

So what impact do budget decreases have on IT security? 14% said that it will force them to switch to cheaper products (30% last year), 11% said that they would reduce IT security staff hours (again, 30% last year). For those suggesting they would reduce IT staff or hours 22% were from the US. Only 5% said that a decreased budget will make them outsource their IT services, mainly from mid-sized organizations based in Mexico and Germany. 28% said they would eliminate or reduce their purchase of new security products, 40% said the same last year. It would seem that budget savings are being spread across the range of possible security expenditure.

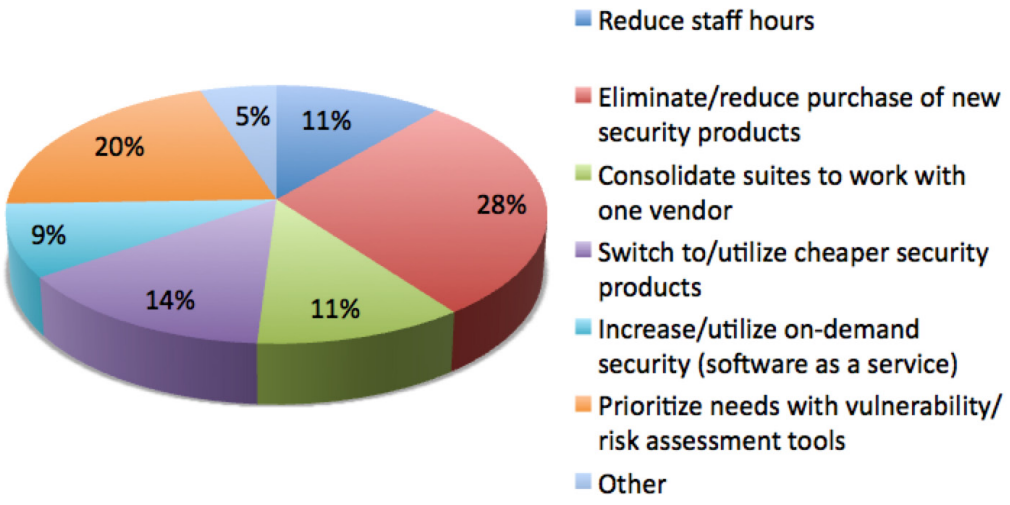

Figure 7: What measures do you expect to take in 2010 as a result of the budget decrease?

Costs and budgets

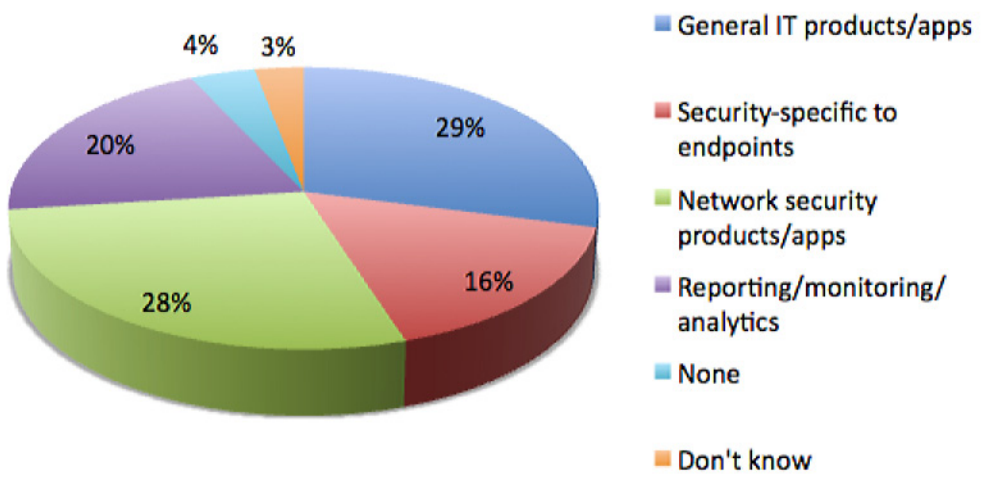

Figure 8: What areas are critical for you to consolidate?

Asked what products they would consolidate with one vendor, 29% selected general IT products and applications and 16% selected security specific endpoints.

Outsourcing of services is still an important part of the security mix but, interestingly, 27% of respondents still refuse to follow this route. Across all regions the training of IT staff is the most popular outsourced service and mid-sized organizations in LTAM are more inclined to outsource their troubleshooting and fine tuning than any other region. On-site administration is most popular in North America, in particular the United States.

Despite the poor economy, there are some areas that will see an increase in spending on products or personnel. 15% are increasing spending on network protection and 12% on email protection, such as spam filtering. Areas that are seeing reduced spending—13%—include device protection and tools that minimise the risk of data theft on lost or stolen PCs, laptops and devices.

For each of the security threats or incidents that a company has experienced there is an associated cost.

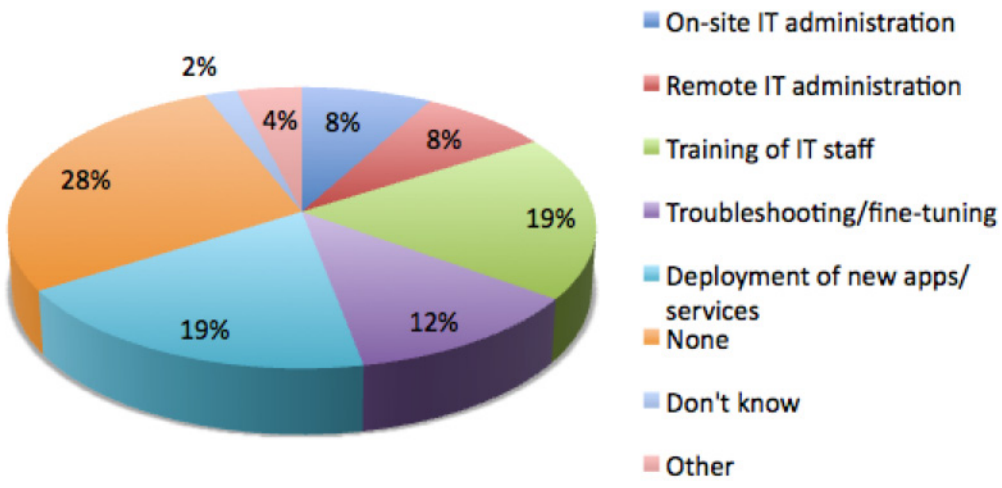

Figure 9: What services do you outsource?

Costs and budgets

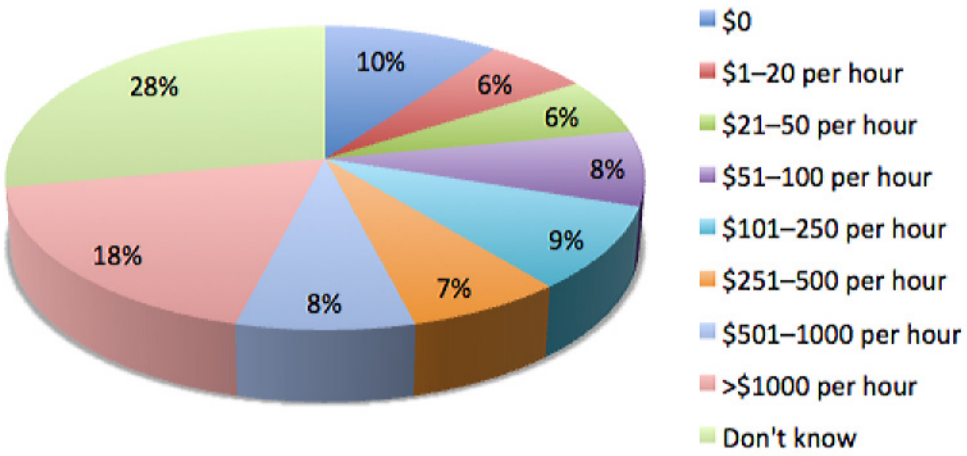

Figure 10: Please estimate the hourly cost of network downtime (in US dollars)

Respondents were asked to estimate the US dollar value they would place on the cost of recovering from an individual incident of malware infection on one PC. 10% estimated the cost to be between $1–20, rising to 3% who estimated the cost to be in excess of $1000. Clearly the value of data on the PC was high, or the organization may legitimately take the decision to scrap it all together and not bother with a fix at such a high cost.

Network incidents can be notoriously expensive, measured on a dollar/hour cost, especially in a mid-sized organization with limited resources. Of those surveyed, the costs were fairly evenly spread from a few dollars through to $1000 per hour but, for an unfortunate 18%, they had costs in excess of $1000 per hour for a network incident.

Respondents were asked to estimate how much it had cost to fix and recover from a typical incident over the previous year. This is a cost per incident and needed to include factors such as products and services, downtime, IT man-hours to remediate the problem, and so forth. For those incidents costing over $1000, 19% were related to the loss of a device and sensitive data leaving an organization. The cheapest incidents to fix and recover from were those relating to email and malware attached to messages.

Summary: Building a proactive defense

In order for mid-sized organizations to rebound, remain competitive or thrive, they are building out areas of their business: enabling a mobile workforce, leveraging cloud delivery options or creating new markets using Web 2.0 applications. For each of those business enablers, IT has to ensure the right processes and policies are backed up by the right security infrastructure and the right training and engagement with their staff, partners and customers.

Achieving this balance is difficult, as we have seen from this year's Paradox survey. Attention to detail is crucial when it comes to IT security spend and sweeping budget reductions across the board are no longer appropriate due to the variety of threats organizations face.

So what should mid-sized organizations do today?

1. Insist on getting real-time threat intelligence to help stay ahead of dangers.

2. Look for vendors who streamline the process of security management to help reduce the time spent on manual processes.

3. Develop internal policies and approaches that ensure each threat vector is covered in some way.

4. Look for multi-layered security solutions, for example those that combine anti-virus protection with data encryption, so that they are not having to solve each security issue with a standalone product.

These intelligent, focused activities will enable any mid-sized organization to defeat the security paradox once and for all.

Terminology and definitions

A number of terms and phrases were used during the data collection phase. These have been defined as follows:

- A security incident is one in which there was downtime, a data breach or a data loss that was unintentional. For example the loss of a laptop, USB stick or file inadvertently attached to an email.
- A security attack is an intentional attempt at compromising system or network security. For example a 3rd party destroying or stealing data, stealing devices, or shutting down a system or network.
- A data loss is defined as sensitive data leaving an organization either accidentally or intentionally.
- Device loss is defined as a device that is lost or stolen whilst containing sensitive data.
- Endpoint protection is the prevention of all types of malware on PCs and laptops.
- Email threats are malicious programs or pieces of code attached to email messages.
- Web site threats are phishing and hacker attacks against an organization's web properties.
- Network security threats include network hacking and unauthorized network intrusions.
- Application code threats are security vulnerabilities (either intentional or unintentional) found in software code that has been developed internally or sourced from 3rd parties.
- Database security and monitoring is the detection and prevention of targeted attacks against database systems, for example SQL Injection attacks.
- Mobile security includes breaches of voice and data content on mobile (cell) phones.
- Cloud-based services include security breaches associated with cloud-based applications.
- Intellectual property includes designs, patents, formulas, software and other similar material of value to an organization.

Further Information

Further information about this subject is available from http://www.BloorResearch.com/update/2055

Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organizations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organizations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

About the author

Nigel Stanley
Practice Leader—Security

Nigel Stanley is a specialist in business technology and IT security and now heads up Bloor's IT Security practice.

IT security comprehensively covers the whole remit of protecting and defending business or organizational systems and data from unwelcome attacks or intrusions. This large area includes protection from the outer edges of the security domain such as handheld devices through to the network perimeter, inside threats and local defences. It looks at the ever-growing threats, many of them new and innovative. It includes use of fire walls, data loss prevention, data encryption, anti-malware, database protection, identity management, intrusion detection/prevention, content management/filtering and security policies and standards.

For a number of years Nigel was technical director of a leading UK Microsoft partner where he led a team of consultants and engineers providing secure business IT solutions. This included data warehouses, client server applications and intelligent web based solutions. Many of these solutions required additional security due to their sensitive nature. From 1995 until 2003 Nigel was a Microsoft regional director, an advisory role to Microsoft Corporation in Redmond, which was in recognition of his expertise in Microsoft technologies and software development tools.

Nigel had previously worked for Microsoft as a systems engineer and product manager specializing in databases and developer technologies. He was active throughout Europe as a leading expert on database design and implementation.

He has written three books on database and development technologies including Microsoft .NET. He is working on a number of business-led IT assignments and is a principal consultant with Incoming Thought Limited, a partner company to Bloor Research that specializes in security consultancy and education.

Nigel is a member of the Institution of Engineering and Technology, the British Computer Society and the Institute of Directors.

Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com