State of Security

EVALUESERVE
YOUR GLOBAL KNOWLEDGE PARTNER

McAfee®
An Intel Company

CONTENTS

1 Executive Summary

Information is intrinsic to the core of any business. Most organizations would find it impossible to function without the availability and absolute privacy of their proprietary – and priceless – information. Therefore, securing it across the extended enterprise is critical to the success of any organization.

Every organization needs to take a layered approach to security, utilizing both processes and solutions designed to prevent compromise. Complicating the challenge of managing risk and securing data is the fact that "the enterprise" now extends far beyond what were the traditional boundaries of enterprise networks and perimeter firewalls. Companies are giving direct network access to trusted business partners and contract workers, and in some cases, even to customers. Workers access the enterprise network remotely using consumer-class mobile devices, many of which are personally owned and not controlled by the company whose network they access. Moreover, data and applications are being moved into public and hybrid cloud environments where the data owners have little direct control over security.

As the corporate infrastructure expands beyond the traditional network perimeter, we believe that effective information security is possible only on the basis of a sound Strategic Security Plan (SSP) which incorporates a comprehensive threat analysis and an in-depth layered security risk mitigation approach.

As the corporate infrastructure expands beyond the traditional network perimeter, we believe that effective information security is possible only on the basis of a sound Strategic Security Plan (SSP).

To better understand how organizations manage the planning and securing of their digital assets, McAfee, Inc. retained Evalueserve to conduct an independent assessment of how organizations manage their security policies and processes, and what threats are perceived to pose the greatest risk to their business. This global study highlights how IT decision makers view the challenges of securing information assets in a highly regulated and increasingly complex global business environment. It is also forward-looking, revealing companies' IT security priorities around processes, practices and technology for 2012.

This study does not address the effects of compliance with industry and governmental regulations, but McAfee's recent "*Risk and Compliance Outlook 2011*"[1] study specifically highlights the impact of compliance on security and should be considered a complementary piece of research:

"The focus on risk and compliance management comes at a critical juncture as companies are under considerable pressure to protect customer information and privacy, and sensitive business information (business plans, intellectual property, etc.) against threats from cyber criminals, competitors, and even hostile governments. These pressures have intensified as national and regional governments, industries, and in some cases, business partners require increasingly tight compliance in implementing and enforcing IT policies, processes, and controls around key assets and sensitive information. Most companies have to deal with multiple regulations and no business sector is exempt from this."

An update to the above mentioned study is currently underway to highlight trends for 2012, and is expected to be out in the first quarter of this year.

Given the current threat outlook, and the ever-changing technology, regulatory and compliance environments, companies cannot afford to let their guard down by curtailing their investment in security and risk management solutions appropriate for the information security infrastructure.

Definitions and Demographics – Security Maturity

The participants were asked to categorize their organization's overall "Security Maturity" posture. Moreover, the survey delved deeper into individual risk management and security areas to extract a composite picture of individual areas of strengths and weaknesses within the organizations surveyed.

[1] Risk and Compliance Outlook 2011
http://www.mcafee.com/us/resources/reports/rp-risk-compliance-outlook-2011.pdf

The "Security Maturity" categorizations help us understand the mindset of the companies as they view enterprise information security. The terms below are used to describe the level of security maturity of participating organizations:

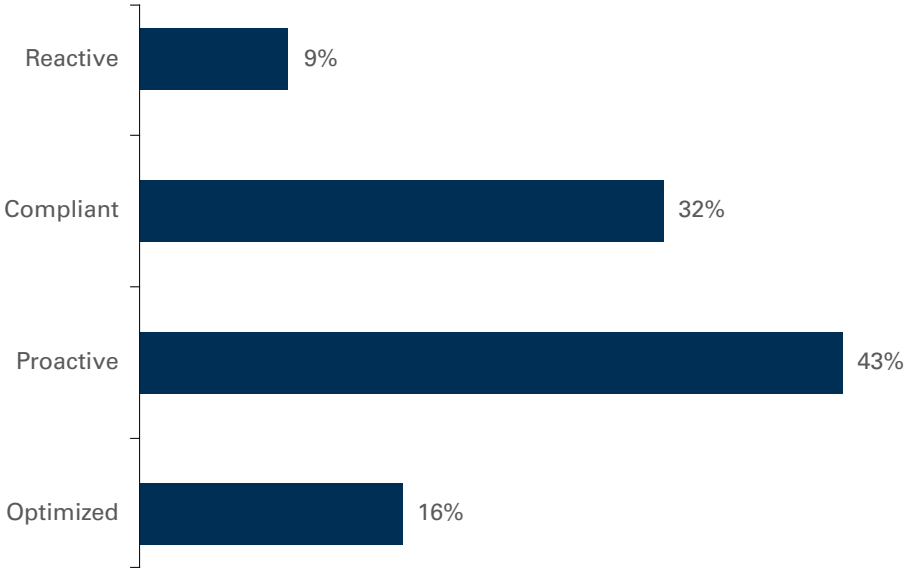
Reactive – uses an ad hoc approach to defining security processes and is event driven. ***9% of the surveyed companies claim to be at this stage.***

Compliant – has some policies in place, but has no real standardization across security policies. The organization adheres to some security standards or the minimum required. ***32% of the surveyed companies claim to be at this stage.***

Proactive – follows standardized policies, has centralized governance, and has a degree of integration across some security solutions. ***43% of the surveyed companies claim to be at this stage.***

Optimized – follows security industry best practices and maintains strict adherence to corporate policy. The organization utilizes automated security solutions which are highly integrated across the enterprise. ***16% of the surveyed companies claim to be at this stage.***

Figure 1: Organizations' Overall Security Maturity



Source: Evalueserve Primary Research

Key Research Findings

1. Organizations are confident about identifying the most critical threats to their environments and knowing where their critical data resides. Contrary to this assertion, most companies are not confident about quantifying the potential financial impact of a breach, should one occur.
2. Organizational awareness and protection against information security risks is very important. However, one-third of the "*Optimized*" companies are uncertain about their IT security posture in terms of awareness and protection. Despite having formal strategic plans, many companies believe they are not adequately protected against information security risks.
3. A majority of the respondents tell us that as they develop Strategic Security Plans, they include consideration of potential threats and the associated risk to business and financial analysis.
4. Almost a third of organizations surveyed have either not purchased or not yet implemented many of the next generation security technologies that are designed to address current-day threats.
5. Most organizations identify malware, spyware and viruses as major security threats. This indicator suggests that organizations recognize the pervasiveness of cyber criminals' attempts to compromise their environments.
6. Top priorities for 2012 include implementing stronger controls to protect sensitive data and ensuring business continuity. The lowest priority is to reduce capital and operating expenditures for security infrastructure.

2 Strategic Security Planning

All of the companies in this survey are taking what they consider to be the appropriate measures to mitigate security risks to their business. However, despite their planning and risk mitigation efforts, 79% of the surveyed companies experienced some type of significant security incident within the past year that resulted in financial and/or reputational impact. This tells us there is still room for improvement in developing, implementing and executing a sound Strategic Security Plan (SSP).

The SSP is a complex collection of activities that support information protection of the organization. This plan involves technology, formal management processes, and the culture of an organization. A SSP is a layered management tool that is the foundation for an organization's information security program. It is about creating, operating, and managing effective risk-appropriate controls.

Need for a Strategic Security Plan

As the world of electronic commerce evolves, a security strategy should focus on building business trust relationships where the relationship itself is based on little more than data passing through a network. The increased scope of information sharing between organizations also requires an increased focus on protecting this information from unauthorized use or exposure. But, protecting shared information is more than simply restricting access to authorized users. It requires an in-depth layered approach to security.

The trustworthiness of the information, as it supports business transactions, must be established and maintained. Many times management looks past technical security issues and assumes that only internal staff will be accessing the systems, and that physical and administrative controls will compensate for inadequate technical security. With organizations opening their systems to external parties such as vendors, customers, and sometimes even the public at large, this creates the potential of negating previously implemented controls.

To maintain the trust relationships organizations and their extended user base rely upon, a dynamic integrated system of controls is required. These controls should be specifically designed to manage known technical and business risks at hand.

The following are interesting observations about the surveyed companies and their security plans:

- Two out of every five organizations have either an informal or ad hoc plan or no strategic security plan in place at all.
- The size of the organization matters when it comes to having a formal SSP. Six of every ten large enterprises have a formal SSP, two out of every three mid-size enterprises have a formal SSP, while this ratio dips to only one in two small enterprises.
- Organizations in North America and Germany are more likely to have a formal SSP than those organizations in other regions of the world. This may be attributed to the regulatory environments in those countries.
- More than half of the organizations that claim to be at the "Compliant" security maturity level do not have a formal SSP. This is not surprising, because this study defines a "Compliant" organization as one that" adheres to some security standards or the minimum required." Though having a SSP may not be a standard, especially if the respondents' companies are not publically traded / regulated organizations, a SSP would be considered by many security experts a best practice.

Time Span of the Strategic Security – How Far Out to Plan?

Considering the rapid changes in technologies and the type of threats that companies face, a majority of organizations (77%) create security plans focusing on the near future ranging up to two years. The rest of the organizations (23%) build their plans to cover a time span longer than two years. Additionally, one-fourth of mid-sized and large organizations have plans that span more than 2 years.

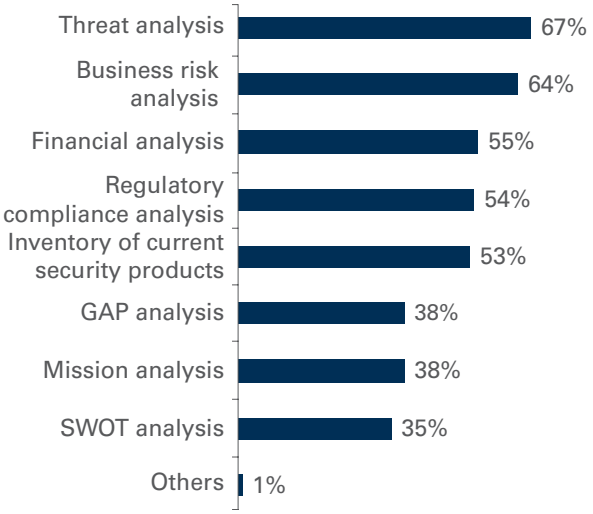
> 79% of the surveyed companies experienced some type of significant security incident within the past year that resulted in financial and/or reputational impact.

Security plans developed by European and North American companies have an intermediate focus of six months to two years as compared to companies from South America which differs significantly with short term security plans that span less than six months. Also, more companies that are "*Optimized*" in their security maturity have a longer term view in their SSP, with plans that typically span more than three years. Companies at lower security maturity levels tend to have shorter term plans—if they have a plan at all.

What are the Elements of a Strategic Security Plan?

When asked what elements comprise the respondents' SSP, about two-thirds say they include a threat and business risk analysis (see Figure 2). Approximately half include a financial analysis, regulatory compliance analysis, and an inventory of their current security products. Only 38% of the companies include a gap analysis which would outline the "security holes"— the areas where there is deemed to be insufficient coverage for the perceived threats and business risks.

Figure 2: Elements of Strategic Security Plan



	United Kingdom	North America	Germany	France	Australia & New Zealand	Singapore	Brazil
Threat analysis	76%	71%	39%	86%	67%	71%	60%
Business risk analysis	83%	71%	49%	38%	74%	74%	59%
Financial analysis	56%	62%	49%	57%	62%	52%	48%
Regulatory compliance analysis	58%	58%	55%	61%	58%	58%	32%
Inventory of current security products	56%	52%	58%	61%	49%	47%	46%
GAP analysis	41%	42%	29%	43%	35%	41%	35%
Mission analysis	48%	48%	33%	36%	35%	42%	21%
SWOT analysis	42%	29%	33%	12%	38%	50%	40%
Others	1%	1%	1%	0%	1%	0%	0%

Source: Evalueserve Primary Research

Only 38% of the organizations include a mission statement in their plan. An effective mission statement clarifies the purpose and aim of the SSP, and provides a road map in guiding an organization during a security breach. More than 50% of organizations, who perceived themselves as "*Optimized*" in security maturity, do not have a mission statement or a SWOT (Strength, Weakness, Opportunity, and Threat) analysis in their SSP. Even though these organizations may have a strategic plan there is room for improvement to elevate their plans to make them much more effective.

Who Creates and Validates the Strategic Security Plan?

Designing, developing and implementing an effective SSP and the related strategic security objectives of an organization are complex, arduous tasks which require leadership and ongoing support from executive management to succeed. Also, developing a security plan requires the involvement and commitment of business unit managers, process owners, finance managers, risk and compliance officers, as well as the IT and security management teams.

As might be expected, response to the question "*Who participates in formulating and validating the strategic security plans?*" shows the involvement of personnel from the IT department (78%) and the security team (63%) in designing their security strategies. Only 40% of executives and general managers get involved, and often their participation is largely during the final decision making stage. Responses to this question, however, may be a factor of the respondents' point of view; people in a decision making role indicate more involvement of executives and general managers compared to respondents in other roles.

Organizations that are at an "*Optimized*" security maturity level would be expected to be more structured and organizationally inclusive in their approach toward security planning. This was validated with 52% of "*Optimized*" companies having involvement of executives in the development and validation of their SSP. As expected, this is a higher participation rate than companies in any other phase of maturity, with participation rates of 32% in "*Compliant*" organizations; 36% in "*Reactive*" organizations; and 40% in "*Proactive*" organizations.

Keeping the Strategic Security Plan Up-to-Date

The discipline of IT security is quite dynamic with new and continually evolving threats, and vendors making technological advancements to mitigate them. Organizations must remain both vigilant and current with their understanding of the changing paradigms

> Only 38% of the companies include a gap analysis in their SSP.

to assure their security plans are effective at mitigating the risks '***they are not willing to accept***'.

To that end, once implemented, an organization's security plan cannot be viewed as a static monolith of achievement. It's important that the plan's performance be continually monitored to assure that risk mitigation objectives are being achieved. Further, when threats emerge that cannot be mitigated with the current approach, adjustments are required to both the approach and plan.

Analysis of the survey results indicates that nearly two-thirds of the organizations update their security plans on a monthly or quarterly basis, while 13% update them on an ad hoc basis as the need arises. This observation is consistent across the various countries and the company sizes in the survey.

Companies that are at an "*Optimized*" and "*Proactive*" maturity level tend to update their security plans on a regular basis, typically quarterly. Companies with informal plans are more likely to update them, such as they are, as needed on an ad hoc basis.

Strategic Security Plan

Need for Survival

22% ↑

August 2011 McAfee Threats report: First half of 2011 the **busiest in malware;** 12 million malware samples – **22% increase** over 2010.

APWG, Phishing Activity Trends Report 2011: Data Stealing & Trojan malware reached an **all-time high** in first half of 2011, comprising almost half of all malware detected.

64%

Ponemon Institute, State of Endpoint Risk Study 2011: 64% organisations acknowledged networks are **not more secure** compared to 2010.

79% !

McAfee Sep. 2011 State of Security Survey: 79% organisations experienced significant security incident in the past **12** months.

Organizations with Formal Strategic Security Plan (59%)	Organizations without a Formal Strategic Security Plan (41%)
21% organisations are Optimized and 45% are Proactive	Only 9% are Optimized
49% are well aware and well protected against IT security risks	Only 15% feel they are well aware and protected
39% high on confidence about gauging the right financial impact of a breach	Only 28% are confident about gauging the right financial impact
44% with Formal Plan are highly confident about deployment of countermeasures to protect critical information assets	Only 20% are confident around deployment of countermeasures
Organisations with Formal Plan are more open on use of new age technology like Application Whitelisting (61%) and Next Generation Firewall (62%)	Lesser proportion (45%) use any next generation technologies
Only 4% do not rehearse incident response scenarios	17% never rehearse incident response scenarios

Not having a Formal Strategic Security Plan puts organizations into a more reactive mode....

Optimized organizations	Average data loss impact	Reactive organizations
$581, 937		$1,106,137

Optimized organisations with Formal Strategic Security Plan are twice more capable of handling malware and security breaches!!

3 Management of Security Policies and Procedures

An integrated security plan is about how all the elements – people, policies, procedures, technology, architecture and corporate culture – are effectively aligned to enable a company to do what would be otherwise too risky. It's not solely about technology; it's about all of these elements working together to support a measurably effective business strategy.

The survey participants were asked to describe their organization's information security processes and practices; in other words, the security maturity level we defined earlier. Keep in mind that *Optimized* is the highest level of maturity, followed by *Proactive*, then *Compliant*, and finally *Reactive*.

The largest percentage (43%) of respondents identify themselves as being "*Proactive,*" meaning the organization follows standardized policies, has centralized governance, and has a degree of integration across security solutions. These practices certainly help increase awareness and the organization's security protection posture, but there is still room for improvement to reach the highest level of security maturity.

> It's an unfortunate reality that many security teams struggle to keep up with the soaring volume and sophistication of threats.

Knowledge and Awareness of Security Risks and Security Solutions

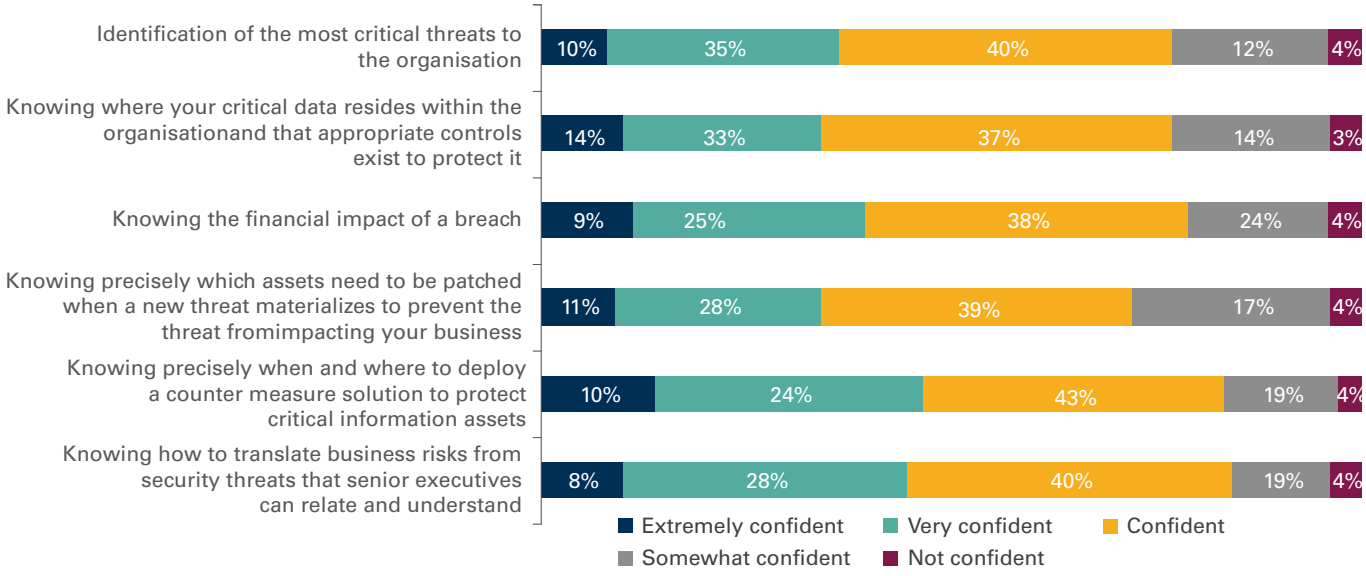
It's an unfortunate reality that many security teams struggle to keep up with the soaring volume and sophistication of threats. This can be attributed to many factors, not the least being a lack of understanding of the ever changing threat vectors. This challenge in understanding threat implications is a difficult yet important requirement in risk management, especially as organizations extend their business operations around the world, and beyond the 'enterprise'.

Every day organizations are faced with an increasing number of threats. While hackers and malware are attacking from outside the perimeter defenses, disgruntled trusted insiders or social engineers may be circumventing security from within.

Timely detection, clarity and understanding of the severity of threats, and the ability to implement timely mitigation strategies, help keep businesses out of the line of fire from both internal and external threats.

Figure 3 highlights the level of confidence organizations have in identifying threats, translating them into business risks, knowing which assets would be affected, knowing how to mitigate the risks, and understanding the potential financial impact a threat brings to an organization.

Figure 3: Knowledge about Security Strengths and Solutions



Source: Evalueserve Primary Research

In contrast, the next figure (Figure 4) highlights organizational awareness of threats, the appropriate protection against threats, and their associated security risks. Three out of four companies believe they are aware of the security risks that they face, but only about a third of the companies believe that they are both aware and well protected.

Risks of Extending Network Access to People and Places

Many enterprises extend network or application access into their partners' offices, trusted insiders' homes and other off-premise locations. Carefully controlled and managed access to a company's internal network is imperative regardless of the user's location and relationship to the company hosting the network.

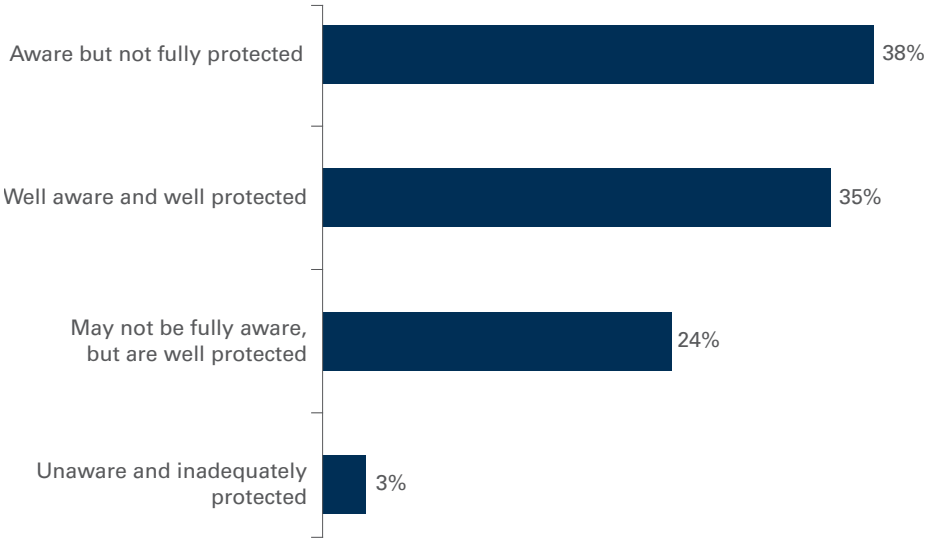
- 83% of all organizations indicate they allow employees and internal users access to their internal/corporate network from outside locations.
- 31% of all organizations indicate they allow network or application access to Business/Channel partners. This practice is more common for organizations from North America, the United Kingdom and Singapore, and less so for organizations from other countries surveyed.
- 40% of the self-identified "*Optimized*" organizations allow access to Business/ Channel partners.
- 21% of the organizations allow network or application access to their customers.

The increased flexibility and productivity gained by remote access is accompanied by an increased risk to information resources. The risk can be viewed in three layers: the risk to the computing devices; the risk to the corporate network; and the risk to sensitive data or intellectual property.

Check that Insider!

The insider threat is a unique situation because organizations have both sensitive information and people who have authorized access to it. Even when access to sensitive information appears to be adequately protected, organizations are still at risk because a determined user can still find ways to steal, expose, change or delete information. The challenge is to evolve the layers of information security defenses to better mitigate this exposure.

Figure 4: Awareness and Protection against Information Security Risks



Source: Evalueserve Primary Research

According to the report *Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector*,[2] a collaborative initiative of the U.S. Secret Service National Threat Assessment Center (NTAC) and the CERT® Program of Carnegie Mellon University's Software Engineering Institute (CERT):

> Estimates of how often government agencies and private companies are victimized by illicit cyber activity from within are difficult to make. It has been suggested that insider incidents are under-reported to law enforcement and prosecutors. Reasons include insufficient damage to warrant prosecution, insufficient evidence to prosecute, and concerns about negative publicity should reports of the incidents surface.

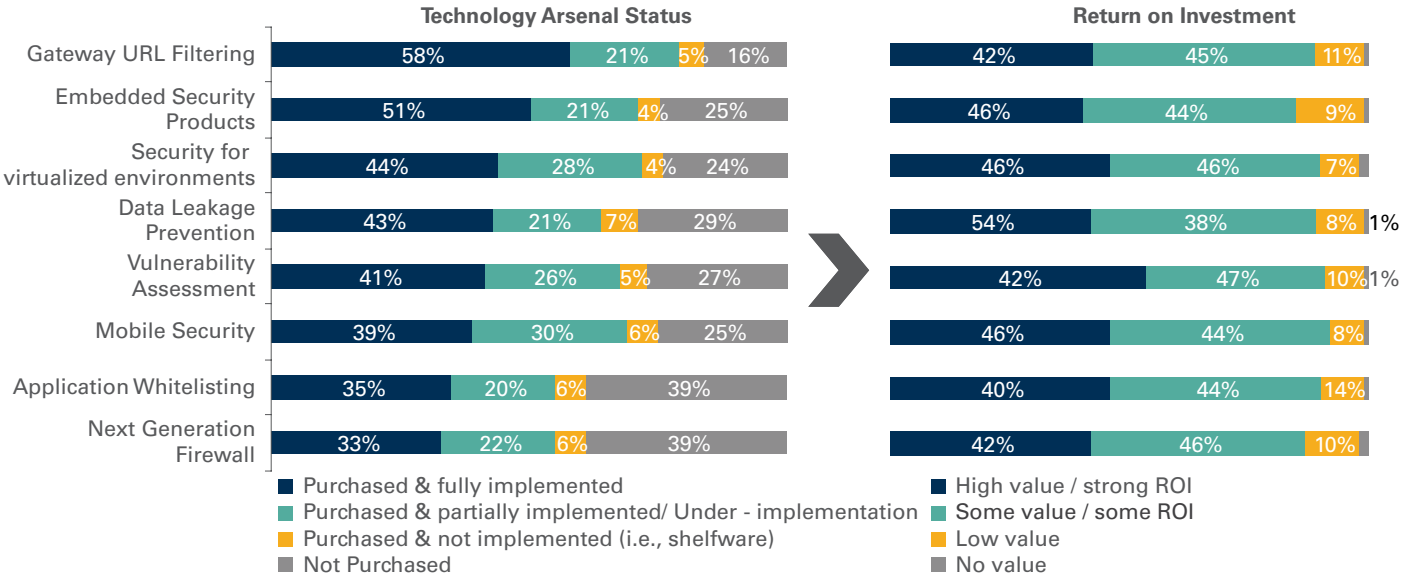
Occasionally the breach of trust by an insider makes the news. Wikileaks is a prime example. The question arises, why are these leaks and thefts, at a minimum, not detected and, ideally, prevented? The simple answer is that information security practices have generally not been refined to look for the unwanted activity of a trusted insider. The technology exists to identify and potentially prevent this activity, but it must be implemented to do the job. The survey also shows that 68% organizations have identified the insider malicious activity as threat in their SSP but only 48% of them have addressed it.

Security Technologies – What Companies are Buying and Using

Examination of the survey results around a variety of technologies shows which ones are most likely to have been purchased and implemented, and which technologies have not been purchased due to individual organizational considerations (see Figure 5). For example, Next Generation Firewalls, which allow for very granular policies for individual users' access to web applications, are least likely to have been purchased and deployed.

[2] Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector, January 2008, http://www.secretservice.gov/ntac/final_it_sector_2008_0109.pdf

Figure 5: Technology Arsenal Status and Return on Investment



Source: Evalueserve Primary Research

Surprisingly, approximately 30% of the organizations surveyed have either purchased and not implemented, or not purchased security technologies that better enable layered security strategies. These technologies include Embedded Security Products, Security for Virtualized Environments, Data Leakage Prevention, Mobile Security, Application Whitelisting, Vulnerability Assessment and Next Generation Firewall. Paradoxically, most of these organizations associate some degree of value with these technologies.

Budget Allocation for Security Measures

Information security is a delicate balance between minimizing risk while managing cost. Most of the companies in the survey allocate between 11% and 14% of their annual revenue to their total IT budgets, and of this budget, 10% to 14% is allocated to information security efforts.

This allocation is in line with a recent Gartner report, *User Survey Analysis: 2012 Security Buying Behaviors and Budget Trends*,[3] where it highlights:

> Last year's budget expectations were for a 6 percent share of the total IT budget expenditure to be allocated to the security function. In this year's survey, that allocation has increased to a mean of 10.5 percent, an increase of over 4 percent.

In reality, the concern is not whether IT security expenditures are higher or lower than the average; it is more important to determine if it is needed and justified. David Lello, a director at Gartner Consulting says, "*It's possible to spend a fortune on security, but if it's done poorly, it doesn't help a business.*"[4]

Good planning helps make the most of what budget is available. Not surprisingly, the survey shows that organizations that self-identify as being "*Reactive*" in security maturity, generally expend more of their budget on resolving security issues. This increased spending is due to an absence of an overall security plan that defines risk-appropriate security policies. As a result, these organizations spend most of their resources on combating threats and recovering from issues because they do not have appropriate security policies in place.

Using Metrics to Measure the Performance of the Strategic Security Plan

Security metrics are generally used to measure how well an organization is meeting its security objectives as defined by the security plan. Metrics are particularly helpful in identifying trends over a period of time by tracking performance and directing resources so that they can initiate performance improvement actions.

[3] Gartner, "User Survey Analysis: 2012 Security Buying Behaviors and Budget Trends"
[4] IDG News Service, "How much should you spend on IT security?", September 22, 2010

According to the SANS Institute publication *A Guide to Security Metrics*:[5]

"Good metrics are those that are SMART, i.e. specific, measurable, attainable, repeatable, and time-dependent, according to George Jelen of the International Systems Security Engineering Association. Truly useful metrics indicate the degree to which security goals, such as data confidentiality, are being met, and they drive actions taken to improve an organization's overall security program. Distinguishing metrics meaningful primarily to those with direct responsibility for security management from those that speak directly to executive management interests and issues is critical to development of an effective security metrics program."

There are three key factors that drive the need to measure IT security performance: financial, organizational, and regulatory.

- Financially, using metrics for measuring successes and failures of past versus current security investments helps organizations justify and direct future security investments.
- Organizationally, accountability to stakeholders ensures an appropriate level of mission support, determines IT security program effectiveness, and improves customer confidence.
- Regulatory is done to demonstrate compliance with a particular law or mandate.

How Often Companies Analyze and Report Their Performance

Slightly more than 60% of the organizations surveyed say they analyze and report on the performance metrics to management on a weekly (33%) or monthly (28%) basis. Further, organizations across geographies tend to report performance on a weekly basis. Larger enterprises prefer reviewing and reporting performance both quarterly and monthly. Against this backdrop, smaller enterprises generally analyze and report performance monthly.

Twenty percent of "*Reactive*" and 17% of "*Compliant*" organizations analyze and report performance metrics to management when needed or requested compared to 5% of "*Proactive*" and "*Optimized*" organizations. Companies with informal/ad hoc/no strategic plan appear to be more erratic in reporting performance metrics to management.

Reporting the Company's Security Posture - What to Report?

Dynamic IT environments and organizational requirements make the process of evaluating, developing and managing a company's information security posture very complex. Communicating the security posture to executive management in an easy-to-understand manner is actually an even more complex task because of its technical nature.

> A larger number of "Optimized" companies compared to those at any other security maturity level report performance metrics to senior executives.

The challenge is how to present, in easy to understand terms: the mapping of security solutions to business risks; the explanation of the overall security strategy and its supporting security plan in detail; and a *gap analysis* of security and compliance issues.

The survey shows that more than one-quarter of the organizations from Singapore and Brazil rank mapping of "*security solutions to business risks*" as the top method to describe their information security posture to management. This is compared to approximately 10% of organizations from North America and France that do the same.

Figure 6 highlights the respondents' priorities in describing security posture to executive management.

Reporting the Company's Security Posture – Who Needs to Know?

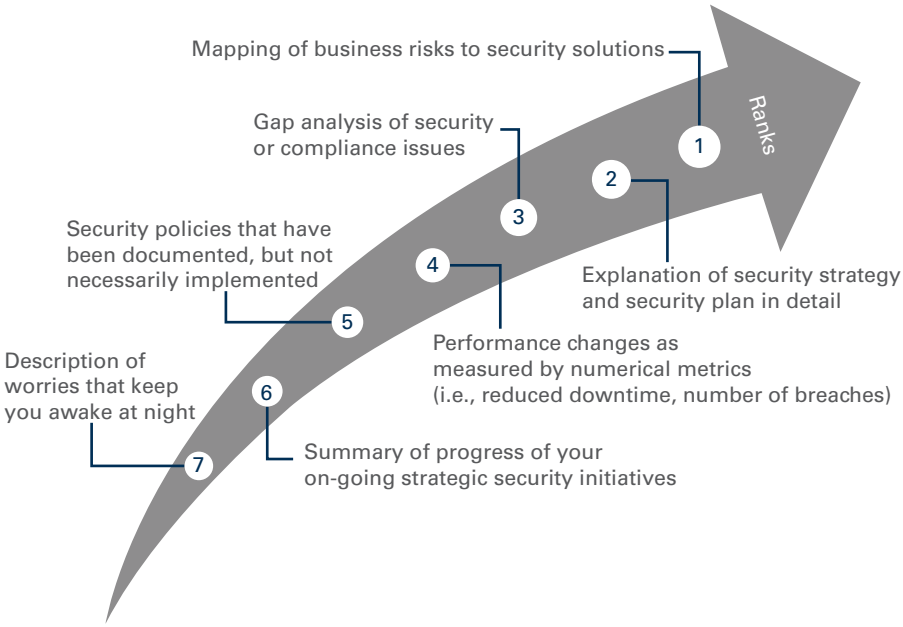
The main IT security stakeholder can be anyone within the organization, but traditionally that role resides with either the CIO or the CISO.

A larger number of "*Optimized*" companies compared to those at any other security maturity level report performance metrics to senior executives. Companies with informal/ad hoc/no strategic security plan involve more departments in reporting metrics as compared to companies having a formal security plan, understating the belief that these companies may operate in a 'fire-fighting' mode with an 'all-hands-on-deck' approach.

Also, 35% of the organizations say they present security performance metrics to their Board of Directors.

Each stakeholder is being presented a set of metrics that provides a view of the organization's IT security performance within that individual's purview. This implies that metrics-related roles and responsibilities are dispersed throughout an organization. The challenge is to select the most appropriate and critical elements of the organization's IT security program for management reporting.

Figure 6: Priorities in Describing Information Security Posture to the Top Management



Source: Evalueserve Primary Research

[5] SANS Institute, A guide to Security Metrics, Shirley C. Payne, June 19, 2006

4 Security Threats

The security threat landscape continues to shift, grow, and evolve. Not only are attacks carried out by highly motivated external sources that target specific industries or organizations for financial gain, now, organizations must also account for the so-called trusted insider that may steal, expose, or delete sensitive information.

Threats have been identified but are they being addressed?

As mentioned earlier, one of the top IT security priorities for 2012 is the implementation of stronger controls to protect sensitive data.

As shown in figure 7 below, approximately 79% of the organizations surveyed indicate that data loss, malware/spyware/ viruses, unauthorized access, outside attacker, and remote access as primary security threats in their security plans. Among the respondents, only 59% indicate that these threats are addressed with a clear approach within their plans.

Secondary threats such as denial of service, weak authentication, social engineering, and natural disasters are identified in 62% of the security plans, while only 42% of them have a clear approach to address these secondary threats.

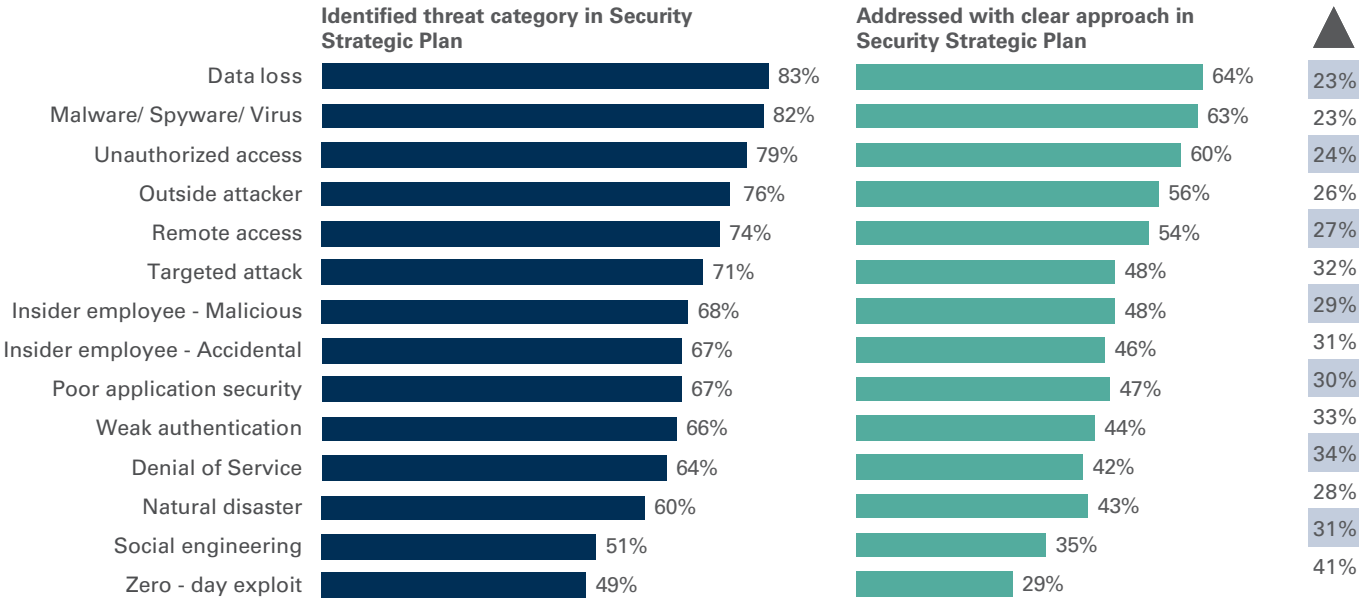
Overall, this shows a large gap, of more than 20%, in threat identification compared to a clear approach to threat mitigation within the security plans. Regardless of the reasons for these gaps in approach to threat mitigation, these organizations are exposing their IT resources to threats that they identified in their security plans.

Security Starts with Threat Awareness

More than 80% of the organizations surveyed are confident about their ability to identify the most critical threats to their IT resources and know where their critical data resides. These organizations are acutely aware of the risks that they face and believe that they have implemented appropriate controls to protect their critical data and computing resources.

Interestingly, only one-third of the organizations surveyed are highly confident when it comes to their knowledge about the financial impact of a potential security breach.

Figure 7: Threat Vector Categories Identified and Addressed



▲ Difference in terms of percentage change

Source: Evalueserve Primary Research

Figure 8 shows that financial data and transactions, considering their confidentiality and importance to revenue, are the top two enterprise assets that must be protected from security breaches and threats.

Though organizations may be aware of the threat landscape they face, any gaps in data protection can bring reputational, regulatory and legal penalties for them should a breach occur. Data resources are highly sensitive assets that need to be well protected to instil trust and confidence with customers, business partners, shareholders, and government or industry regulators.

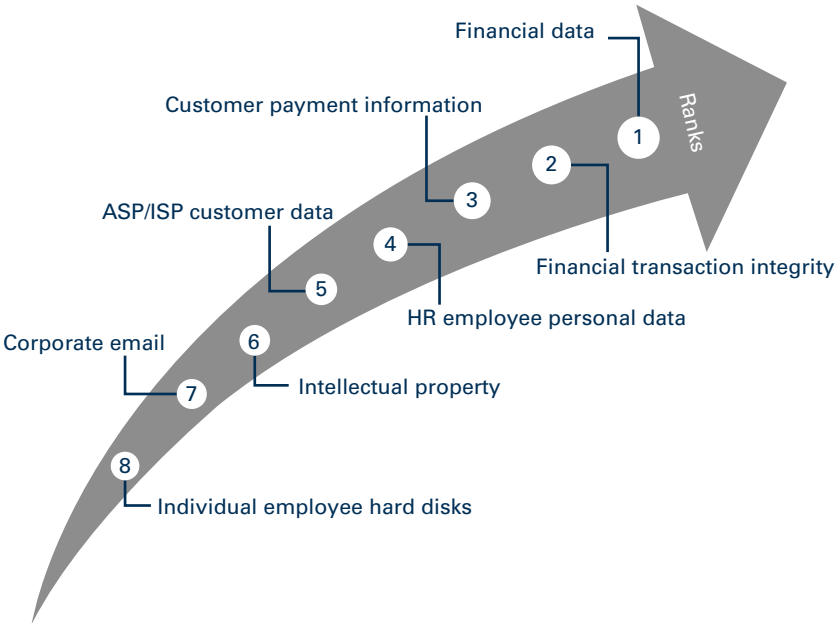
Security Incidents Still Occur

A security incident is a set of one or more security events or conditions that requires action and closure in order to maintain or re-attain an acceptable risk posture. Security incidents come in countless forms and from a variety of vectors. Incidents can affect the availability, confidentiality and integrity of data and processes within an organization in unpredictable ways.

According to the *2010 CyberSecurity Watch Survey*[6], a cooperative effort of CSO magazine, the U.S. Secret Service, Software Engineering Institute CERT® Program at Carnegie Mellon University and Deloitte's Center for Security & Privacy Solution:

"The 2010 CyberSecurity Watch Survey uncovered a drop in victims of cybercrimes (60% vs. 66% in 2007), however, the affected organizations have experienced significantly more attacks than in previous years. Between August 2008 and July 2009 more than one third (37%) of respondents experienced an increase in cybercrimes compared to the previous year. While outsiders (those without authorized access to network systems and data) are the main culprits of cybercrime in general, the most costly or damaging attacks are more often caused by insiders (employees or contractors with authorized access). One quarter of all cybercrime attacks were committed by an unknown source."

Figure 8: Importance of Enterprise Assets



Source: Evalueserve Primary Research

Alarmingly this survey shows as many as 79% of the organizations experienced security incidents in the past twelve months (see Figure 9).

Further examination shows approximately one-fourth of the organizations from France and from North America have reported zero security incidents in the last twelve months. At the same time, 5% of all organizations, and 10% from Brazil, indicate that they experienced more than 26 security incidents in the past twelve months.

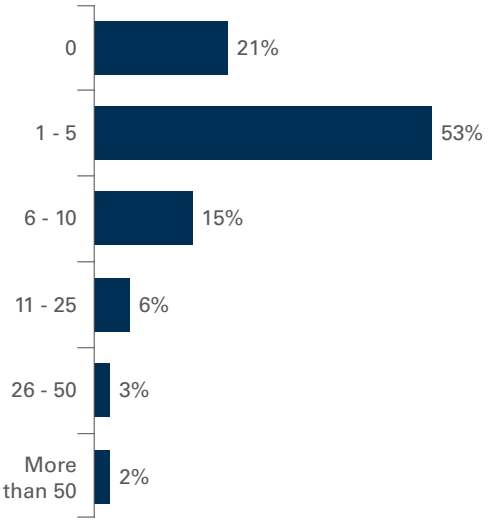
There can be various reasons for these incidents, some of which have already been discussed in earlier sections: No strategic security plan; gaps in identified and addressed threats; and lack of security maturity are few key reasons which stand out.

The Impact of Data Loss

The impact of data loss affects organizations differently depending on the type of loss/breach, how many sensitive records were compromised, and whether or not the information is used to commit fraud. Every organization that experiences a data loss incurs an impact. Financial impact can include direct costs associated with customer notifications, victim remediation services, forensic examinations, fines, lawsuits, and new or updated systems, processes, and procedures. Indirect impact/costs that are harder to quantify may include loss of customer confidence and brand value, and a subsequent decline in stock valuation.

[6] 2010 CyberSecurity Watch Survey, CSO magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, and Deloitte, 2010

Figure 9: Major Security Incidents in the Past 12 months



United Kingdom	North America	Germany	France	Australia & New Zealand	Singapore	Brazil
25%	27%	13%	23%	17%	36%	7%
49%	54%	59%	48%	59%	47%	55%
15%	11%	17%	21%	13%	13%	16%
7%	4%	6%	4%	6%	1%	12%
3%	1%	4%	1%	3%	1%	4%
1%	1%	1%	3%	3%	1%	6%

Source: Evalueserve Primary Research

Of the organizations surveyed, nearly 68% revealed that the financial impact of data loss from recent security incidents was not more than $100,000 (USD). As many as 17% of the organizations from Australia and New Zealand identified impact in the range of $500,000 to $1 million (USD), and at same time only 1% of the organizations from Germany experienced a revenue impact in this range due to data loss.

The cost impact is difficult to compare across geographies, because they may be highly dependent on local laws that require expensive breach reporting and damage restitution for victims affected by the breach. In addition to the revenue loss, 42% of the organizations say they also experienced reputational impact.

Globally, "*Reactive*" companies – those at the lowest end of the maturity scale for information security – acknowledge having the greatest impact of data loss from security breaches, while "*Optimized*" companies reported an average loss of $581,937 (USD)—approximately half the impact value of what "*Reactive*" companies incurred. Clearly there is a financial benefit from being well prepared.

> Despite stating that they are "Compliant," 29% of the surveyed organizations either do not rehearse incident response scenarios after occurrence of a breach or never undertook the exercise of testing their incident response plans.

Crisis Management – How to Respond to an Incident

In order to effectively manage any event that threatens to harm an organization, a crisis management plan and team is necessary. A framework for managing crises should focus on four key areas: containment, analysis, response, and remediation.

To manage such events, it is important that IT organizations have a well tested crisis management plan at the ready. The planning and development should start with identification and education of individuals and systems most likely to be targeted because of their access to important assets. Regular rehearsals of the plan should be performed to test and debriefed to identify gaps in the plan and supporting processes.

Nearly three-quarters of the organizations surveyed rehearse incident response scenarios quarterly or monthly in preparation for breaches. Interestingly, one-quarter of the organizations never rehearse incident response scenarios or do so only after an incident has occurred. Twenty-three percent of the organizations in Australia and New Zealand and 6% of the organizations in North America never rehearse their incident response plan.

Also, as companies progress upward on the security maturity scale they are more inclined to assure their emergency risk mitigation strategies work as planned by conducting tests of their incident response plans.

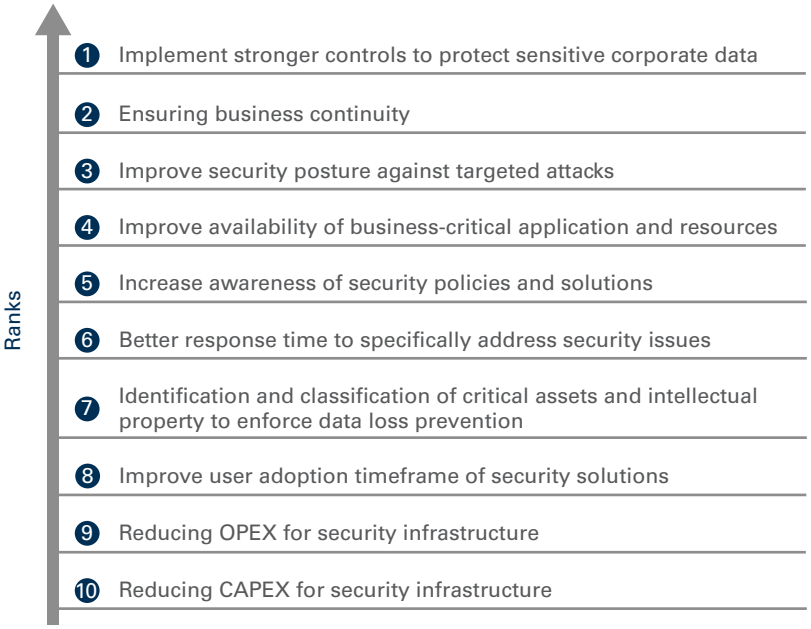
Despite stating that they are "*Compliant,*" 29% of the surveyed organizations either do not rehearse incident response scenarios after occurrence of a breach or never undertook the exercise of testing their incident response plans. Moreover, organizations with a formal security plan display greater prudence in both rehearsing and preparing themselves against any likely breach that may occur.

5 The Focus on Security for 2012

The key concerns and focus for 2012 give significant weight to the implementation of stronger controls that protect sensitive corporate data, and by extension, prevention of targeted attacks (see Figure 10). The research confirms the importance of IT security for any business, and emphasizes that business continuity plans must include recovering from data security incidents as well as from the traditional threats such as fire, flood, and other disasters.

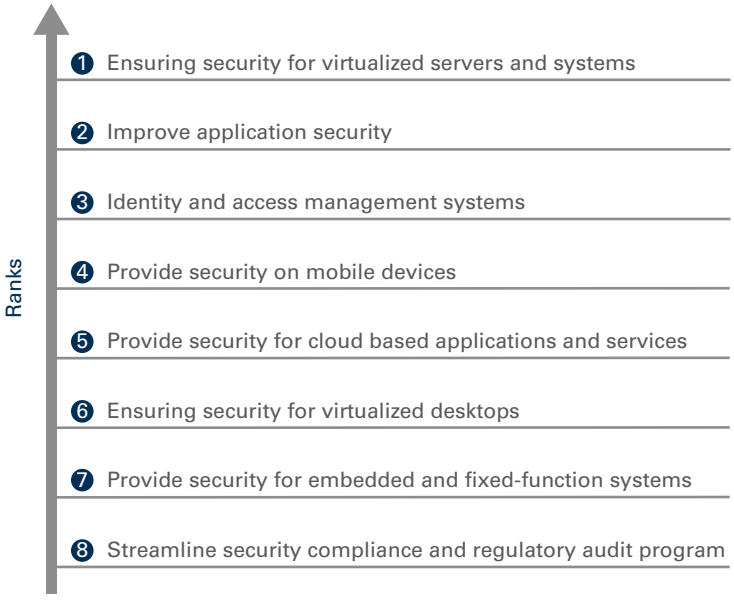
The lowest priority is reducing security infrastructure spending. This is reasonable when considering the potential losses that can be incurred from a security event and the potential impact to business continuity.

Figure 10: IT Security Priorities for 2012 – Process/Practices



Source: Evalueserve Primary Research

Figure 11: IT Security Priorities for 2012 – Technology



Source: Evalueserve Primary Research

The top two technology related priorities include ensuring security for virtualized environments, followed by improved application security.

As organizations rapidly move towards more sophisticated technology processes, ensuring security for virtualized systems and applications is an obvious choice. Enterprises must support hundreds if not thousands of internal and public-facing applications while bringing on new online services to meet customer demands and partner responsibilities.

6 Conclusions

This security survey reveals a glass half empty/glass half full situation. While organizations are working on their strategic security plans and putting in their best efforts toward protecting business systems and critical data, there is much room for improvement all the way around. We can draw the following conclusions and recommendations from the survey findings:

- **Step up to a higher security maturity level.** A key area for improvement would be for organizations to take the steps necessary to increase their level of security maturity. Only 16% of the survey respondents classify their organizations as being at the "*Optimized*" level. Worse, however, is the fact that 9% of the organizations are "*Reactive*" in their approach to IT security. Organizations may have a Strategic Security Plan but there is also room for improvement to elevate the plans to make them much more effective. Ideally organizations need to follow security industry best practices and standardized policies, and have centralized data and security governance.
- **Executive involvement is crucial.** Our survey reveals that, for the most part, organizational involvement is good when it comes to developing the Strategic Security Plan. While IT and security personnel may take the lead in developing the plan, it is important to have the line of business (LOB) leader's insight to understand business risks and the information assets they use. Moreover, executive involvement is critical to set the tone for the importance of security throughout the organization. Good security starts at the top when the senior executives say, "This is important to the well being of our enterprise and everyone must keep our information assets secure."
- **Test early, test often, and make adjustments as needed.** What good is a plan if it is developed and put on a shelf? If it is never tested? How can the organization know if the plan will even be effective in a crisis? Organizations need to regularly test and adjust their plans as needed to adapt to new and emerging threats. Unfortunately we learned that 29% of "*Compliant*" companies never test how they would respond to an incident. What's more, the fact that 79% of the surveyed companies had security incidents in the past year indicates that there are holes in the security plans that must be addressed.
- **Use budget allocations wisely.** We see that funding for IT security is adequate, and even in these tough times, there's little interest in cutting the security budgets. Though every manager would like to have a bigger budget to be able to apply more safeguards, the "*Optimized*" companies have found ways to reach the highest level of performance with the same level of funding (percentage-wise) as the companies who are less prudent with their budgets. The "*Optimized*" organizations have learned that investing in sound preventative measures is less costly than paying for remediation. In contrast, "*Reactive*" organizations spend more time and money than necessary taking care of problems after they arise than trying to prevent them in the first place.
- **Use the right tools for the current threats.** As threat vectors continue to evolve and grow next generation security tools should be evaluated and implemented with a risk-based approach that is part of the overall security strategy. For example, many new threats are coming into organizations via the Internet. Previous generation firewalls leave too many openings for new threats to enter the enterprise network without scrutiny. Still, the survey shows that 45% of the companies haven't deployed the next generation firewalls. Mobile security is another area that should not be ignored, yet 25% of the organizations have not purchased any tools for this purpose.
- **Focus on protecting the lifeblood of the company-the sensitive corporate data.** The top priorities for 2012 include implementing stronger controls to protect sensitive data and ensuring business continuity. Additional high priority activities are all meant to improve each organization's overall security posture. This is encouraging because without timely recognition and mitigation of security threats, an organization may be the next news headline—and nobody wants that dubious distinction.

7 A Glimpse of who participated and what we asked

The survey included responses from 495 respondents from organizations representing a wide spectrum of industries such as Manufacturing, Education, Technology, Government, Healthcare & Pharmaceuticals, Retail and Financial Services. These organizations cover four geographic regions:

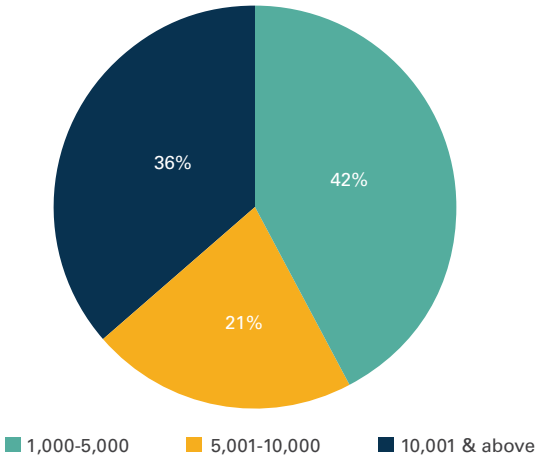
- North America: United States and Canada
- Europe: United Kingdom, Germany and France
- South America: Brazil
- Asia/Pacific: Australia, Singapore, and New Zealand

They range in size from a minimum of 1,000 employees to more than 50,000 employees. The size demographics are as follows:

- 42.3% of the companies surveyed are Small Enterprises, with between 1,000 and 5,000 employees
- 21.4% are Medium Enterprises with between 5,000 and 10,000 employees
- 36.3% are Large Enterprises, with more than 10,000 employees

The survey includes responses from IT decision makers, consultants, and security analysts involved in the evaluation, selection, day-to-day management and maintenance of IT security processes and solutions.

Figure 12: Organization Size Break-up

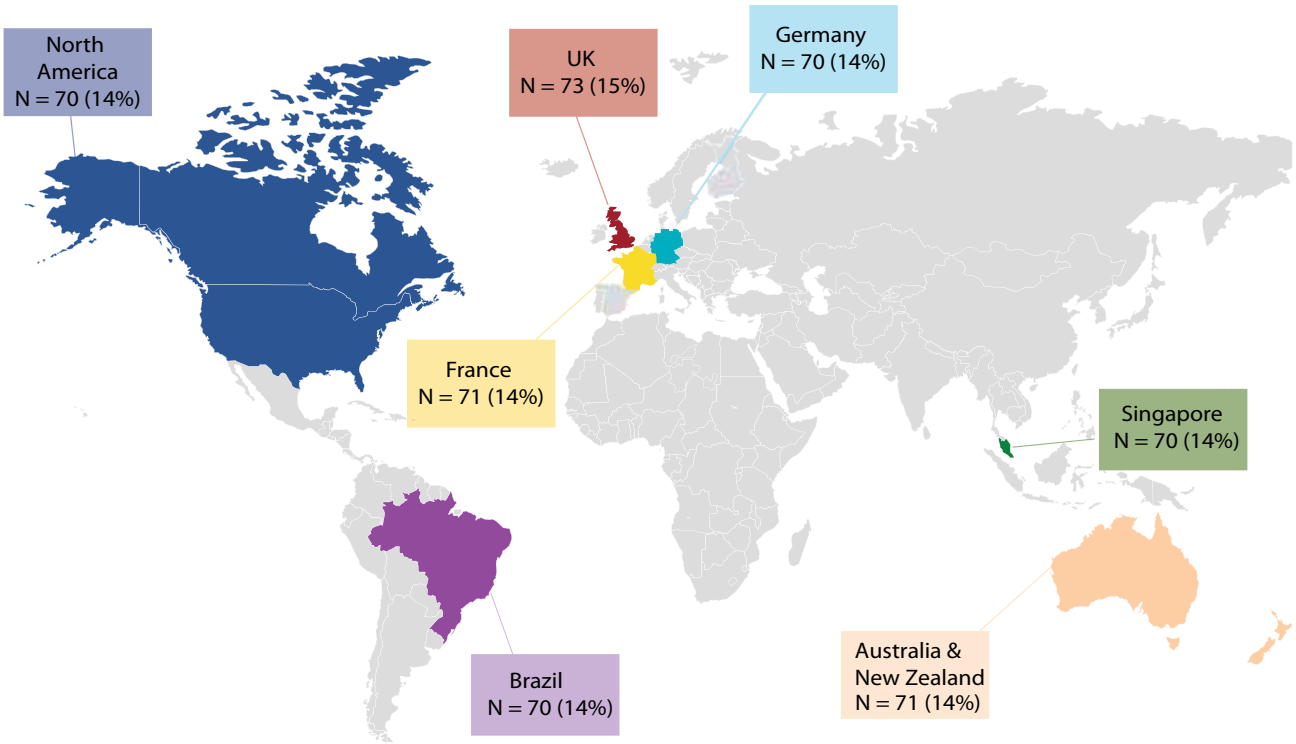


Source: Evalueserve Primary Research

The survey consisted of 32 questions designed to help us answer the following key questions:

- What processes are followed to build a Strategic Security Plan?
- What are the business roles that contribute to developing the plan?
- What do security decision makers do with the plan after its creation?
- What is the process that Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) go through to analyze threats?
- How do the security decision makers prioritize the threats that need countermeasures?
- Is there an understanding around how new threats impact the organization?
- Is there a formalized way to review security controls and their capabilities?
- How do organizations test and measure security controls for effectiveness?

Figure 13: Regional break-up of interviews



About Evalueserve

Evalueserve is a global specialist in knowledge processes with a team of more than 2,600 professionals worldwide. As a trusted partner, Evalueserve analyzes, improves and executes knowledge-intensive processes and leverages its proprietary technology to increase efficiency and effectiveness. We have dedicated on-site teams and scalable global knowledge centers, in Chile, China, India and Romania, which provide multi-time-zone and multi-lingual services.

Evalueserve's knowledge solutions include customized research and analytics services for leading-edge companies worldwide. By partnering with us, clients benefit from higher productivity, improved quality, and freed-up management time. We provide our clients with better access to knowledge and information across all parts of their organization, thereby adding to their capabilities.

EVALUESERVE
YOUR GLOBAL KNOWLEDGE PARTNER

McAfee®
An Intel Company