

I NTRODUCTION

Security spending is one of the few areas that is strong in an otherwise weak economy. Enterprises and government agencies are spending an average of 10% of their IT budgets on security initiatives. Security software and services account for over 50% of the spending planned for 2003. CSO Magazine reported in January 2003, that over a third of the companies it surveyed had security budgets in excess of \$1 million. It's easy to see why so many vendors are launching security practices and products lines.

But what about the customers?

Is all the spending netting the expected ROI?

Are security vendors delivering on their promises?

Are customers really feeling more secure?

We set out to explore those questions this winter. Our goal was to understand the challenges enterprises face as they work to protect their systems, their employees and their businesses.

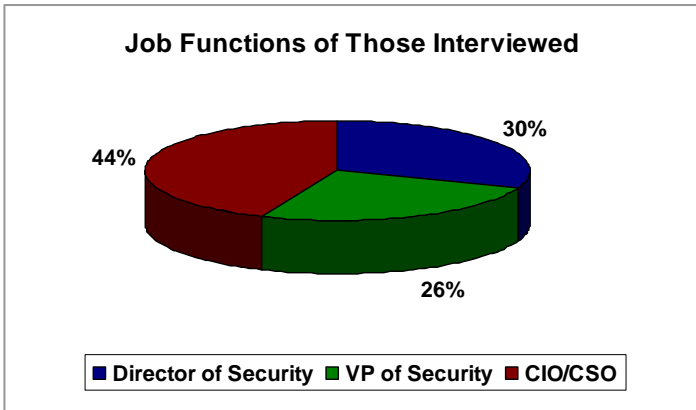
Our research revealed, while security executives have improved visibility and have to fight a little less for budget dollars, security has yet to be fully integrated into the business. Executives continue to struggle to:

- Implement policies and hold users accountable
- Develop rationale risk assessment models
- Balance security against worker productivity
- Protect the business while enabling collaboration with customers and suppliers

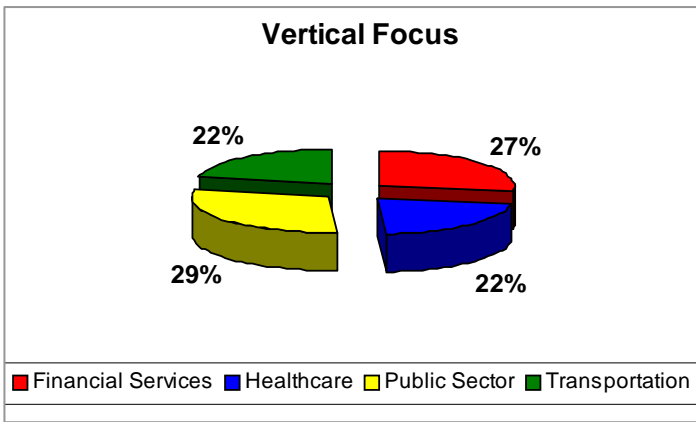
The purpose of the paper is to explore:

PURPOSE, SCOPE, & METHODOLOGY OF THIS STUDY

- What enterprises and public sector agencies view as their top accomplishment and priorities in security since September 11, 2001
- How integrated is security planning across the enterprise
- What enterprises and public sector agencies see as their most pressing challenges in security
- What Best Practices are employed by enterprises and public sector agencies

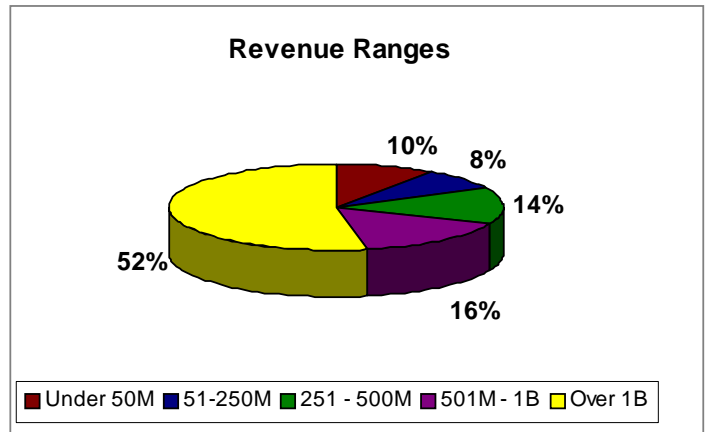


AZtech obtained the information for this study through a series of qualitative telephone interviews ranging from 45 to 90 minutes each. AZtech interviewed 36 Global 1000 companies and 15 Public Sector Agencies in North America, the UK and Europe from late November 2002 through January 2003.



Interviews targeted CXOs whose responsibilities include at least two of the four primary security areas. For the purposes of this paper, these areas are defined as cyber, financial, physical, and operational.

In 93% of the companies, CIOs or CSOs participated in the screener. In 56% of interviews, the CXO referred AZtech to an appropriate staff





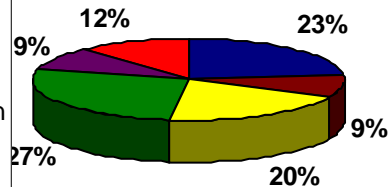
ACCOMPLISHMENTS

Immediately following September 11, 2001, security executives focused heavily on improving or developing disaster recovery plans. Security in financial services, transportation and the public sector verticals also became very much about regulatory compliance.

This, for many executives, created an opportunity to focus on policy development and building end user awareness. The new regulations touch so many components of the business outside of IT, that for the first time, executives were able to develop overarching policies that also improve the strategic positioning of security in their organizations.

These policies seek to place programs such as compliance, privacy and business continuity in the context of a holistic approach to security. Although most admitted their organizations still don't necessarily treat security holistically; executives insisted at the user level, people must understand not only the regulations, and what they need to do to be compliant, but why compliance was important to the business as a whole.

Accomplishments



Security executives, especially in financial services and the public sector, felt security awareness has traditionally been a challenge because it's handled as a discrete event rather as part of a holistic strategy. According to respondents, the key to an effective security program is the grass roots understanding of corporate objectives. Too often, the technology component is the focus and users lose sight of their role.

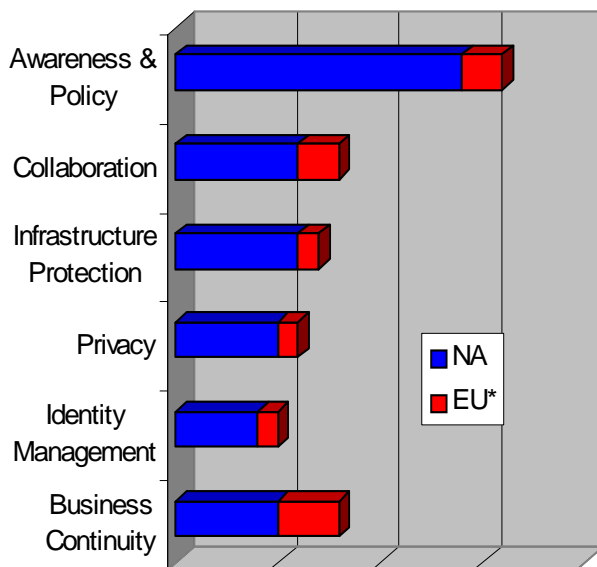
Unfortunately, policy implementation continues to be one of a security executive's greatest challenges.

Infrastructure protection is another area where security executives feel they've made measurable improvements. Over 75% of executives cited their handling of the Nimba/Code Red viruses as evidence their infrastructure is significantly more secure than two years ago. However, all felt they still had room from improvement especially as it relates to maintaining a secure environment while extending the enterprise to better collaborate with customers and partners.

P RIORITIES

As they look to 2005, security executives continue to focus on increasing end user awareness. 87% state end user awareness of the security implications of their actions remains very low. 43% are implementing structured training programs for employees. However, 78% of those have yet to succeed in integrating security compliance into employee performance reviews.

Security Priorities



To be honest, I think the flaw if anything is with people like myself and other people with security responsibilities for not selling this in the right way. We need to sell security to our senior management as actually adding value as opposed to restricting what people can do and what people can't do. - Financial Services, NA

I mean, come on! How many times do you have to get struck by a virus before you learn not to open an email with an executable attachment? It kills me when we send out warnings about a new virus and get it 24 hours later because some idiot ignored the memo. - Financial Services, NA

The biggest single threat, which is actually very, very difficult to deal with, is the internal threat from one's own staff, one's own employees. I think it is the trickiest area and it is probably the one that too often gets filed in the 'too difficult so let's not worry about it' drawer of the filing cabinet. - Financial Services, Europe

Well that's kind of difficult because you can protect the front door, but your real threat is inside, your own people and that's a major education and trying to lock things down if you can but you also don't want to interrupt the job that they have to do. - Transportation, Europe

During the early part of this project, 43% of respondents stated security's rank among the priorities of the business had fallen off over the last year.

However, those interviewed in late January and February expect to see an increased focus on security, especially business continuity, in the board room as the US goes to war with Iraq.

Although the increasing threat of war impacts the immediate priorities of respondents, there remains a strong desire to move away from selling security through fear toward focusing on business enablement, especially as it relates to collaborating with customers and partners.

Too often, security executives stated, they are seen as the purveyors of doom, or worse, inhibitors of growth. As a result, they are often left out business development decisions (e.g. establishing an extranet) until the project is well underway. The net result is increased cost because security is implemented as an afterthought combined with the feeling that once again security is throwing cold water on a "great growth idea." Changing that perception is a personal objective of 78% of those we interviewed.

As stated earlier, respondents cited one of their top accomplishments was the creation of security policies. Policy implementation, however, is one of their greatest challenges. The need to educate executives and users as to their responsibilities and the implications of their actions is a daunting task. The need runs the full gambit from common sense training to the role of security in strategic business decisions.

Our research validated the trends cited in the trades regarding the increasing attention to internal security threats. The most frustrating comes from end user disregard for security policies. The hardest thing to protect against is disgruntled employees.

The constant struggle is to create security programs and policies that protect the organization without impinging on employee's ability to do their jobs. There is also a constant need to rationalize security measures against potential productivity losses.



ASSESSMENTS

Because their role is one of balancing multiple priorities, respondents view outside assessments as critical tools, however, in spite of using them frequently, respondents struggle with the value these assessments deliver. 88% state assessments are a component of their security strategy; but 81% of those are consistently disappointed with the results. Their disappointment centers on:

- Lack of a solid model
- Lack of insight into their business
- Lack of practical application
- Lack of real expertise on behalf of the assessors

Invariably a vulnerability assessment is going to give me a list of stuff that I need to fix, but there is no value from all of this stuff because the consultants don't understand the business. They don't want to spend the time to understand the business. They also don't understand the corporate culture. They don't understand whether the fixes that they give the customer are proportional to the company's need. There is no sort of risk versus reward analysis done on any vulnerability assessment I've ever seen. - **Public Sector, NA**

I'm not seeing what I consider really feasible strategies for continuing to assess the security risk in the business and to present that in business terms. - Financial Services, NA

IT security is amazingly hampered in any industry, because quite frankly, it doesn't have the ability to justify itself properly to rational business people. One of the biggest problems is that there are no proper risk assessment models that actually help good decision making. The models that exist are either too academic or require too many data points where just the collection of the information is extremely expensive. - Transportation, NA

Identifying the gaps is easy. Anyone can do that but identifying whether the gaps should be closed or not is where the rubber meets the road. I haven't met a so called security consultant yet who understands that. - Financial Services, NA

The financial services and healthcare industries in particular struggle with assessments. They are required as a result of the implementation of multiple government regulations requiring the performance of risk assessments. Respondents feel the integration of technology, their business and compliance are extremely complex. However, the assessments they have had to date, fail to adequately address the nuances and complexities. As a result, the final analysis is incomplete.

According to respondents, what most vendors miss is measuring the risk of applying the patch versus the reward of making sure that the company is protected. 68% of respondents cited examples of assessment where the readout offered no remediation. Too often, respondents felt, consultants automatically assumed there were gaps that had to be closed.

Respondents consistently complain assessment models offered by the leading security consultants and integrators do not incorporate security, regulations, business process, decision-making metrics and financial metrics. Over 45% of respondents are actively looking to work with peers, industry associations or vendors to develop better assessment models.

Respondents find it quite ironic that security executives in general are accused by the leading analysts as being short sighted, and for not thinking of their business holistically, when the assessment model analysts tout as Best Practices are guilty of the same short coming.

In general, respondents feel much of what is being offered in the “security solution” space is a result of vendors taking advantage of what they believe is a “hot trend”.



OPPORTUNISTIC VENDORS

Over 50% of the respondents felt like guinea pigs for the vendors.

- Sell what you have, not what I need
- Assessments proved I needed one of their key products
- Claimed to have greater knowledge than they really had
- Didn't take the time to know my business
- Didn't understand the complexity of the regulations

Two themes emerged from our discussions about security vendors:

1. Suppliers (Cisco, IBM, Microsoft, etc) do not think enough about security during product development
 - This was especially true in the public sector in both the US and the UK.
2. Consultants and integrators seem to lack common business sense.
 - All 4 verticals expressed frustration over “holistic models” with no grounding in reality.

In fact, 94% of those interviewed felt vendors who positioned themselves as a “one-stop-shop” were unrealistic. 62% of respondents cited negative prior experience with consultants for why they did not believe in the concept of a “one-stop-shop.” The balance felt, by its nature, security requires multiple vendors.

Vendors, especially the consultant types need to:
1) Get a much better understanding - of my business model and 2). This is the cynic in me; get away from the McKinsey or Accenture business model for businesses. Get to the real world. The impression I get from too many of these people [Consultants] is that they are totally focused on their supposed holistic approach to security, but they rarely leave IT (or never enter it). They need to get out of management school and get into the real world. - *Financial Services, NA*

Realistically, I don't think anybody can do it all. There is simply too much. I don't think one integrator can say "we're going to help you not only lock your doors, but also come up with best practices for how you're going to deal with vendors, secure your data infrastructure, and oh by the way, we're going to help you pick your alarm company, your file storage company, your data maintenance company." I think that's asking for quite a lot, don't you? -
Financial Services, NA

The objections to the "one-stop-shop" messaging from leading consultants and integrators centers around three factors:

1. Volatility of high tech consulting industry as evidenced by:
 - Lack of financial stability
 - Constant consolidation
2. Immaturity of the security field
 - Lack of "mileage" or expertise on the part of the consultants
3. The breadth and complexity of the security space
 - Especially as it relates to compliance and global corporations

As a result, CXOs and their direct reports are reluctant to leverage 3rd parties on security projects. This appears to stem from several sources:

- They aren't quite sure how to tackle the job and are concerned they will not be able to deliver proper oversight.
- They don't trust vendors have the clients' best interest at heart.
- They haven't seen a lot of expertise in the vendors they've used so they're feeling a bit burnt.
- Their decentralized structure and lack of (or newly implemented) policies make it difficult to consistently implement programs or solutions.
- The IT market space is so volatile they have serious concerns about most vendors' long term viability.
- The nature of security makes them want to keep it in house.

S

ELECTION
CRITERIA

Vendor selection criterion in security depends heavily on referrals and references.

Referrals are a common component of vendor selection criteria across all verticals. In order of weight, the chief influencers are:

1. Peers
2. Industry Associations
3. Analysts

Although 81% of respondents subscribe to, or have hired for specific projects, industry analysts, only 33% consider them to be reliable sources of information. Respondents feel the tight vendor relationships the leading analysts maintain is an inherent conflict of interest.

I'm getting too much reactive information from the Analyst community. I'll use [a leading brand] for example. I'll ask them for meaningful information on security risk that we face as a financial institution. What I get, I can read in the newspaper. - **Financial Services, NA**

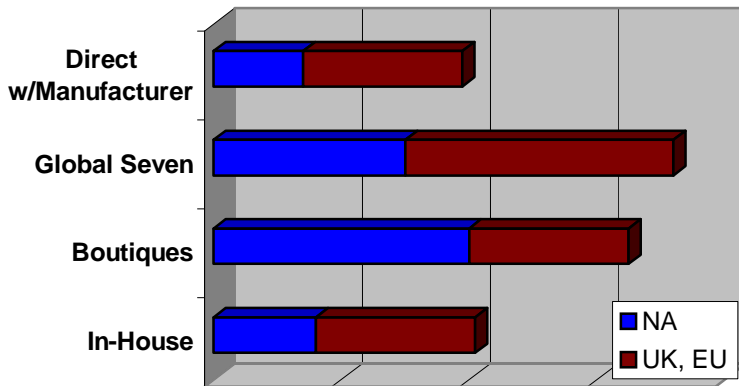
It doesn't matter what the product looks like today - it matters where the product going over the next 3 years, that product will evolve as will the support for it and the capability of inter-operating or adding extra capabilities such working with other management systems perhaps will change over 3 years. So I like to speak to the CEO, I'd like to know where the research is going, I'd like some information on a non-disclosure basis, I'd like to make sure it's got a research team behind it and if it doesn't have a research team it's going nowhere. - **Financial Services, NA**

In addition, enterprises and government agencies who hired an analyst firm for a specific project complain output failed to deliver in-depth forward thinking analysis. 64% of these respondents felt analysts didn't do enough "homework" or that analysts continually pull from the same sources, and as a result do not have solid market intelligence.

For security? My peers... That's my primary source. Sometimes, the Board will ask me what does The Analysts say and I go see The Analyst. But I take everything they say with a grain of salt; most of those guys just write what their clients want them to, but at least I can go back and say here's what I found out. - **Healthcare, NA**

How Does Your Company Handle Security Initiatives?

(*allowed multiple responses)



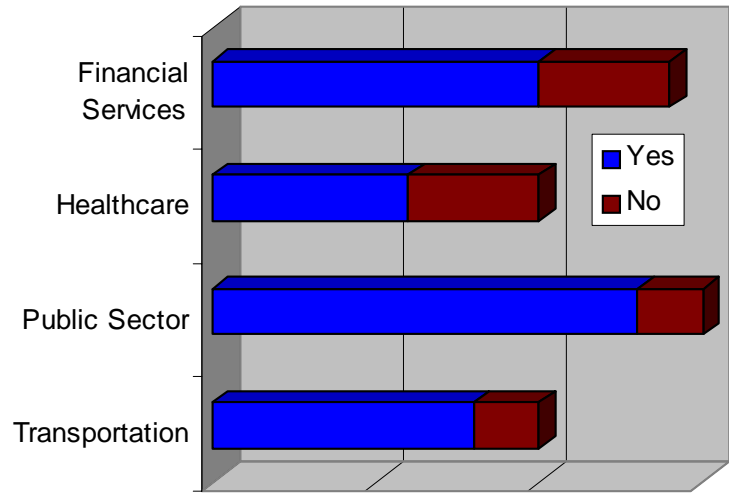
In addition to referrals, respondents evaluate security vendors against the following criteria:

I ask about 5 or 6 questions. One of the questions that I ask is give me one of the toughest situations you've faced, give me one of the toughest customers you've faced, give me one of the situations where you've been successful, give me a situation where you haven't been successful, tell me how much damage you've mitigated and tell me how much damage you've caused. - Public Sector, NA

- Experience -- Respondents concerned about the experience level of the company *and* of the specific individuals who will be assigned to their account
- How stable are they from a human resources and financial standpoint? Respondents also lean toward companies who've been in business for >10 years.
- Will they share their long term technology strategy?
- Do they have knowledge transfer processes/programs?
- Do they have a documented approach?
- What are their vertical strengths?
- Can they deliver local support or continuity of support?

BUDGETS

Is Security Part of the IT Budget?



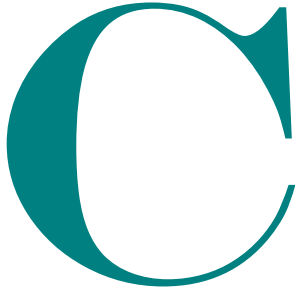
In most instances, the bulk of the Security budget falls under the IT Budget umbrella. It averages 7-10%, however, respondents stated there are other pockets of money throughout the organization being spent on security.

An average of an additional 25-30% comes from other areas, including operations for physical security.

In spite of its increased visibility, respondents are still fighting to maintain budgets, especially in healthcare and transportation. Security executives feel they themselves are often to blame because they have yet to find a methodology for linking security spending and strategic business initiatives.

We've linked challenges and Best Practices because we found respondents shared the same challenges.

However, most feel security still lacks proven Best Practices. We believe we found several Best Practices in the making though.



CHALLENGES & BEST PRACTICES

Respondents articulated six main challenges:

1. Improving awareness and enforcing policy
2. Developing meaningful assessment models
3. Integrating business continuity and disaster recovery
4. Secure collaboration with customers, Partners and suppliers
5. Incorporating new technologies (e.g. PDAs, wireless)
6. Integrating security into the fabric of the business

I can have a great disaster recovery plan. I can have all of the backup tapes, all the rituals there are in the world for having another site up and running within hours, but if we haven't integrated it into a Business Continuity plan, I can see me sitting in a big empty office with a bank of computers all up and running and nobody is left to use them. - **Healthcare, NA**

The challenge I definitely have here is trying to assess the risk of allowing a new product or service to be used versus the exposures that it brings implementing a solution like that with our business units. In other words trying to allow them to maintain their operable ability but still maintaining a secure environment as well. - **Public Sector, Europe**

Best Practices

In the area of those challenges, we found 4 Best Practices:

1. Developing Awareness Campaigns and Enforcing Policy
 - a. Webinars over intranet and extranet
 - b. Publication of audit results as well as self assessment by business units
 - c. Creation of a security coordinator within major departments
 - d. Adding security as a component to performance reviews
 - e. Board level readout of security accomplishments and risk areas with recommendations and implications

I also see as a part of my challenges are advances in technology. How do we incorporate some of those new technologies without giving up security? Such as the wireless and the more frequent use of PDAs ... I cringe with some of the things that they're doing because I know that doctors want to use the handhelds. What if they lose it in the airport? How secure are their Blackberries really? So there are challenges such as that and to make it secure, but yet to have an ease of use-I don't know... it's a balance. - Healthcare,

1. Seeking out peer, association and vendor networking groups to develop assessment models
2. Leveraging scenario planning to demonstrate the outages left by concentrating solely on disaster recovery.
3. Developing and socializing the extended enterprise concept to ensure security is integrated into customer, partner and supplier partnering activities

C ONCLUSION

Security is definitely a top concern, and a solid growth area, but vendors have work to do to meet the needs of their customers. Customers are hungry for forums to share and learn from each other's experience. Vendors have an opportunity to add value and build their own expertise by listening more closely to their customers.

ABOUT AZTECH STRATEGIES, LLC

We believe our value proposition is unique. We adhere to four principles:

JUMP START

We use a “quick strike” approach to projects, providing our clients frequent interim reports and the flexibility to change gears as priorities evolve. Clients leverage our knowledge and our manpower to get ahead of the curve.

CUSTOMER-CENTRIC CHANNELS

Technology will not sell if it doesn't solve a customer problem. We understand which channels enterprises and public sector agencies look to for problem resolution. We realize the support a channel partner can provide to a customer is more important than which manufacturer he represents. We map customer support needs to the type of partner who can meet those needs. We also understand the channel is as much a customer as an end user.

Primary research is our forte. We obtain and validate information for our clients' first-hand or we don't use it.

ACTIONABLE SOLUTIONS

If we don't drive revenue and increase market share for the client and the channel, we haven't finished the job. Ultimately, that's why companies hire us. We are not about ivory tower studies. Rather, we show our clients how to increase market coverage, channel reach and both parties' profitability. We tell clients what their partners and customers really think, who their enterprises and public sector agencies want to buy from and what specific actions they should take to drive more dollars.

We don't just evangelize, though. We roll up our sleeves and work side by side to help our client drive change internally and through channels.

COMPETITIVE DIFFERENTIATION

Innovative thought often reaches farther than the technology itself. We spend thousands of hours a year in conversations with channel partners, enterprises and public sector agencies and manufacturers. We work hard to create strategies and implementation plans differentiating our clients from the pack. Our goal is to make sure our clients win and increase their speed to market. AZtech is personally vested in our clients' success and we look to develop long-term relationships through the quality of our work.

AZtech has been creating new paradigms for channel and partner management since 1996. As the leading channel convergence experts, our officers have 80+ years of product management, distribution strategy and business development experience—all focused on bringing emerging technologies to market. Our ability to see beyond standard verticals and our focus on the fundamentals allows us to offer clients clear, dynamically integrated solutions.