

A 'Trail' of 25 IT Security Heads

We would have assumed that getting information from a IT Security Manager would have been like pulling teeth but the information gathering once we figured out what to ask. If you look at the 100 CIO survey we did in the December 2008 issue, you will be more familiar with the size and budgets that IT departments have available to them, so for this group, we got down to the core issues with the 25 respondents.

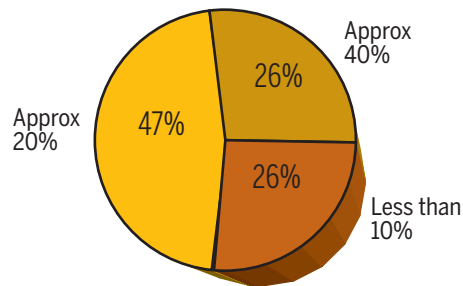
Almost 80% of the people we spoke with, came from the SME-size companies, and in addition to asking about brand recognition of security-related products, we asked them to highlight some of the common mistakes which are made in organization similar to them in size and background and help to identify what the major needs across the organizations was. The objective of asking the questions we did was to assess where the similarities were and how they were being managed.

According to the respondents, some of the common security errors that were being made in most companies included the unethical use of organizational data, virus execution and data theft through the USB and monitoring emails. One of the biggest errors identified by these IT Managers was the fact that most companies copy their IT policies from other companies, usually without customizing any of the policies to fit within their own framework.

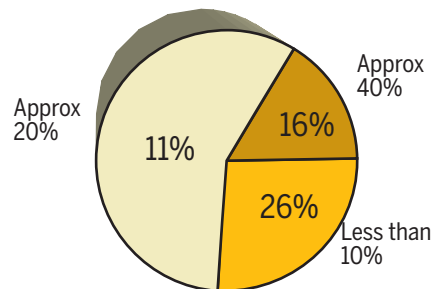
When asked what they thought should be the number one priority of a CSO in an organization, we received replies that included the following: Information Security and Disaster Recovery, adequate control (external and internal), internal threat protection, setting strong IT security policy, enforcing IT security policy, ensuring business continuity and to integrate firewalls and ensuring secure browsing and spam control. Surprisingly, a very small percentage mentioned that it was a responsibility of the CSO to also interact with vendors in the market, or stay updated with security trends or threats.

And not shocking, was the fact that none of the respondents could give a name of a platform or collab-

How much of the company's IT budget should be allocated to IT security?



How much of an SME IT budget would you recommend be allocated to IT security?



The IT budgets, as meager as they seem to be shrinking to, thankfully still allocate a specific portion to security. Perhaps with a greater number of respondents, the percentage allocated for security for a large organization and an SME should balance out to some extent.

orative forum that they were a part of. Knowledge share is almost critical amongst the security managers for the sake of sharing experience and information. Obviously the size of the sample doesn't span the entire breadth of the trend, but much like the trends survey we conducted in the December issue of CMO, this is a start.

Coming to vendors in the market, there seem to be awareness of the major players however we were kind of surprised that even in the random sampling of 25 managers, Juniper was not mentioned and neither was Kaspersky for the enterprise. But then, we're simply accounting this absence to the fact that the sample size was really small, more so for Kaspersky than Juniper, considering there are a limited number of Juniper certified experts and the challenge to get them into Pakistan to work on sizeable projects, becomes a very expensive proposition.

Our objective for asking managers about which brand they associated with the specific type of security-related issue was to simply assess who was considered to be in the market. Over the course of the year, we will be conducting further surveys to better assess the market share each company has within their distinct space, but to be fair, that does require interaction with a much larger population.

It was interesting to note that almost 95% of the respondents were of the opinion that we need a consolidated, national IT security strategy. We might have an IT Policy document, however that is still a distance away from what strategy is required. However more than anything, the IT Security Managers, in their commentary with us, did comment that the market lacked benchmarks against which to rate specific processes and procedures. Because one of the errors pointed out by the managers that a lot of organizations make is taking IT policies from other organizations and trying to implement them within their own company, perhaps a benchmarking system would enable customers to better rate the QoS being generated and offered by a company. [\[10\]](#)

Please note that these responses are only reflective of the data collected by CIO Pakistan and does not place a bias on any vendor cited throughout the course of the survey. In our primary data collection to formulate the survey, the vendor names and percentage ranges were generated by a smaller sample set, prior to opening the survey to the 25 IT Security Managers.

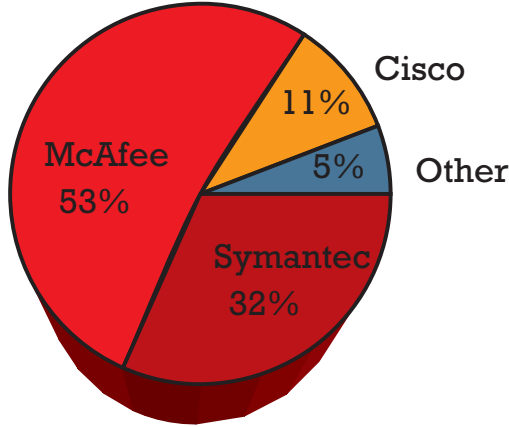
Buzzwords that should be in the CSO's tag cloud

Information Security
Disaster Recovery
Adequate Control **Reliability**
Internal Threat Protection
Unified Threat Management
Secure IT Assets
Penetration Redundancy
Backup
Network Security Intrusion

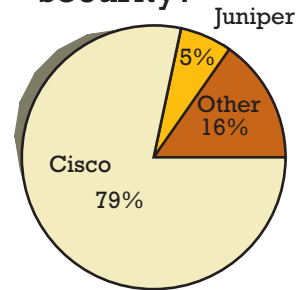
As an IT Security, what kind of threat do you think will do the most damage to your Enterprise?

- USB access
- SPAM
- Data breach
- Viruses and worms
- Poor Network Security Policy
- Hackers and Hactivism
- Lack of contingency planning
- Poor network planning
- Enabling open web browsing
- Accessing P2P software

What's the first brand name that comes to mind when you need consultancy or assistance regarding antivirus?



What's the first brand name that comes to mind when you think IT security?

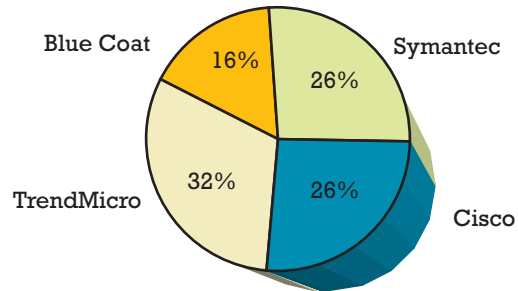


When you think of IT security or IS certification, what certifications come to mind?

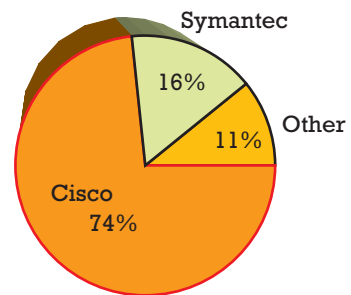
ISO-27001 Certification	26%
CISA	32%
CCSP	37%
CCIE security	21%
Other	32%

Respondents could select multiple certifications which may result in a total greater than 100%

What's the first brand name that comes to mind when you think content filtering?



What's the first brand name that comes to mind when you think of firewall?



Do you think there should be a National IT security policy

