Gabriel CONSULTING GROUP

2011 Data Center Security Survey: Approach & Philosophy

The unrelenting stream of news about security breaches, stolen data, and IT hacking made us curious about the state of data center security these days. With that in mind, we launched our **2011 Data Center Security Survey** (demographics here). Security is part of any data center conversation, of course, but we began to see a need for a top-to-bottom look at all aspects of this vital issue.

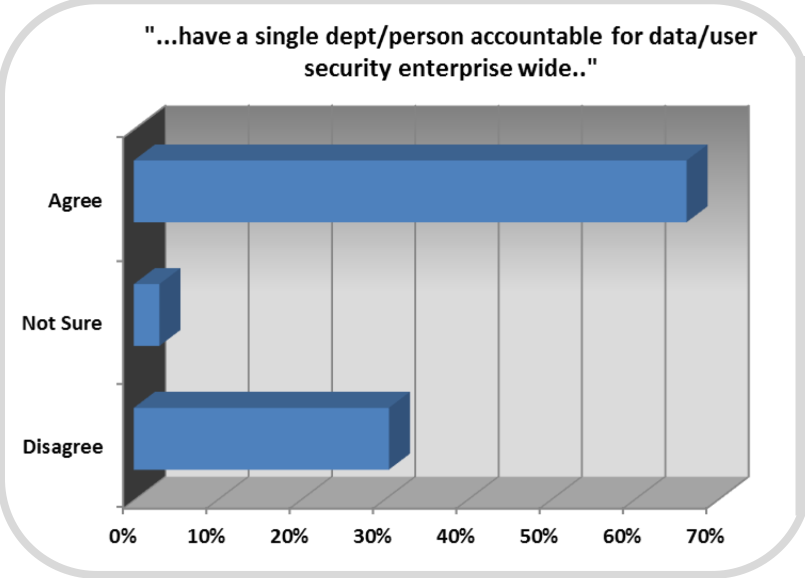
We asked our data center professionals quite a few questions, ranging from their overall approach to security to how well (or poorly) their security is performing; how they've been impacted by breaches; and what they think would help improve their security situation. In this "Approach & Philosophy" report, we examine the survey results that reveal how real-world data centers approach application, data, and user security.

Before the recentralization of IT that virtualization enabled/caused, security tended to be the responsibility of the business unit that owned the application or systems. But the word 'responsibility' was loosely interpreted; often the application owner would throw the system and app over the wall for central IT to maintain and manage.

This led to a situation where the physical systems might be secured from network threats, but the application? Maybe... or maybe not. Security standards for various end-users were fragmented, and the quality depended upon the diligence of the individual business unit.

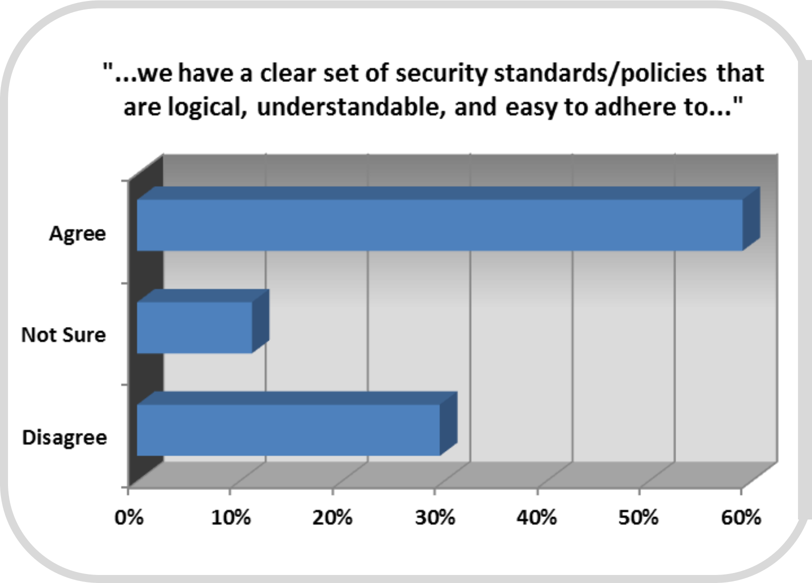
However, the stakes in the security game have increased radically over the past decade or so. There are many more threats lurking, and they're much more sophisticated. In the past, hackers might have been looking to crack into a corporate network for bragging rights; today, there are steely-eyed professionals looking to exploit security holes for profit.

Given this change in the threat landscape, how are data centers approaching security today?



Most organizations have centralized their IT security function – a good step forward, in our opinion. Having a single, enterprise-wide authority on IT security can pay a lot of dividends when it comes to setting up and enforcing security standards.

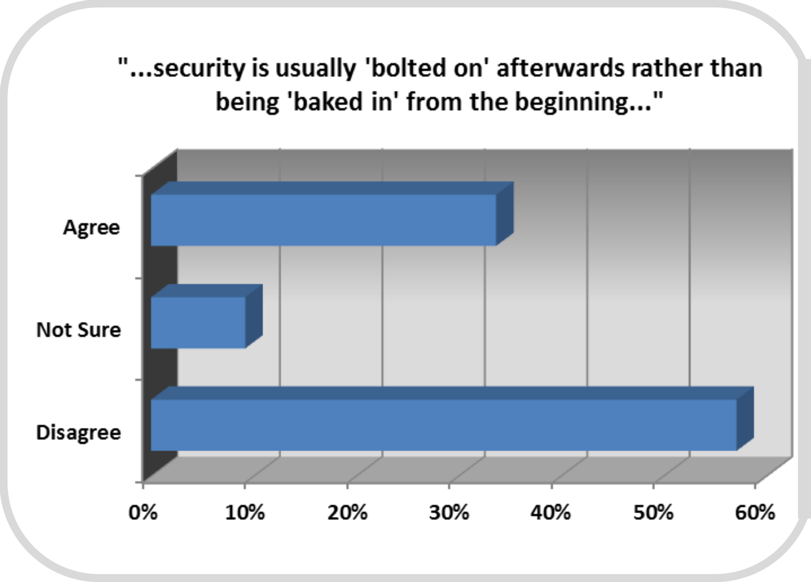
However, simply establishing a central security organization isn't a panacea. This organization can't just be responsible for security; it also has to have the authority to enforce policies. And it also has to be held accountable for security problems that may occur.



"...we have a clear set of security standards/policies that are logical, understandable, and easy to adhere to..."

Plenty of organizations, almost 60%, say that their security policies make sense, are clear, and are relatively easy to live with.

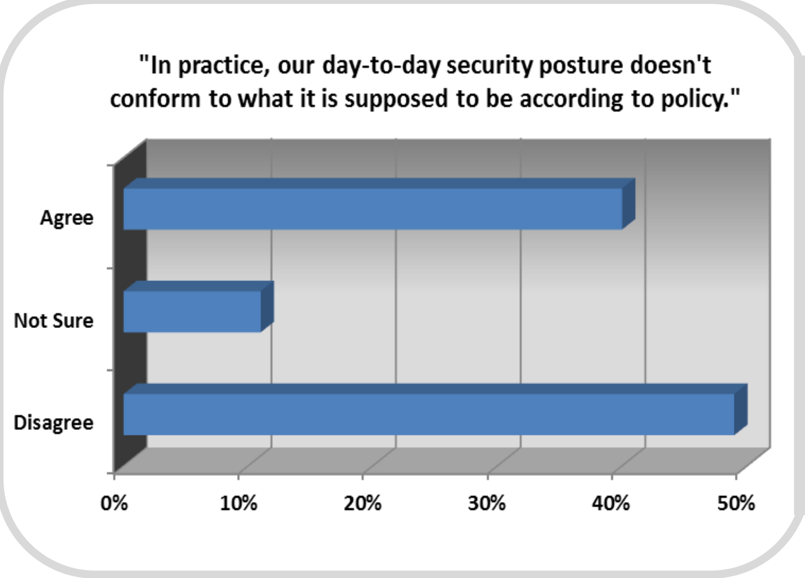
However, there are still 30% of our respondents who say that they don't have these benefits. It's interesting to note that there isn't a strong correlation between the respondents who say that they don't have clear security guidance and those who answered (above) that their security is decentralized. In other words, having a central IT security authority doesn't mean that they'll necessarily do a good job of making security better.



"...security is usually 'bolted on' afterwards rather than being 'baked in' from the beginning..."

Respondents from organizations without a strong centralized security function were somewhat more likely to say that security is 'bolted on' toward the end of a project rather than 'baked in'.

It's easy to see that if more attention were paid to security earlier in the process, the end result would be more secure applications and systems. However, in the rush to get a new project off the ground, security is sometimes reduced to a set of checkmarks on project tracking forms.



40% of our respondents say that their day-to-day security doesn't hit the standards required by their official policies.

Security can be cumbersome at times, and it can prevent IT staff from quickly accomplishing their tasks. There are few data centers that are totally secure all the time, but seeing that 40% routinely operate outside of their security policies is a bit of a surprise. It's a symptom of either poorly thought-out security policies/procedures or IT staff who don't take security seriously enough. Maybe both.

These results are reassuring – well, right up until the last chart above. In general, however, it looks like most organizations are doing the right things: approaching security from an enterprise-wide perspective; establishing clear security standards and policies; and making security an early consideration in their IT projects.

But there's much more to this survey and, as we'll see in our next set of results, there are some reasons to worry if you care about data center security. Even though the majority of users seem to have the right security approach, there are some problems in implementation that are cause for concern. In our next report, we look at how our respondents assess their current security posture – and there are some surprises. You can find that report here.

If you're interested in finding out more about this survey and seeing more results (demographics, expanded results, detailed GCG analysis), click here.

Gabriel
CONSULTING GROUP

www.GabrielConsultingGroup.com
gcginfo@GabrielConsultingGroup.com
(503) 372-9389