# 2011 Data Center Security Survey: Improving Security

The steady stream of high-profile corporate and governmental IT security breaches has placed data center security in the spotlight. The IT security environment today includes a vast array of threats that are constantly evolving in sophistication.

In our **2011 Data Center Security Survey**, we asked data center personnel a wide range of questions about how their organizations deal with IT and data center security. We had 147 respondents from organizations of varying sizes. (Full demographics available here.)

In other sections of this survey, respondents assessed their organizations' current security approaches and the effectiveness of those approaches. They also discussed how they view virtualization and clouds from a security perspective, and even talked about the impact of security breaches on both their main business functions and their data centers. (You can find these results in the Recent Research section of our website here.)

In this final installment, we look at what our survey respondents believe would best help improve their data center security. In the first question, we ask whether reducing the number of security vendors that most organizations have to deal with would be helpful. In the survey, we found that the average mid-sized organization has around six separate security products from an average of four to seven vendors. Is this too much to deal with? Would reducing these numbers simplify security and security management?

Reducing the number of individual security products & vendors we use
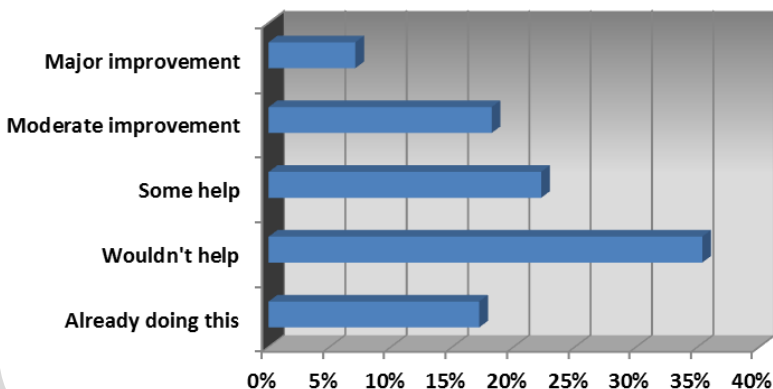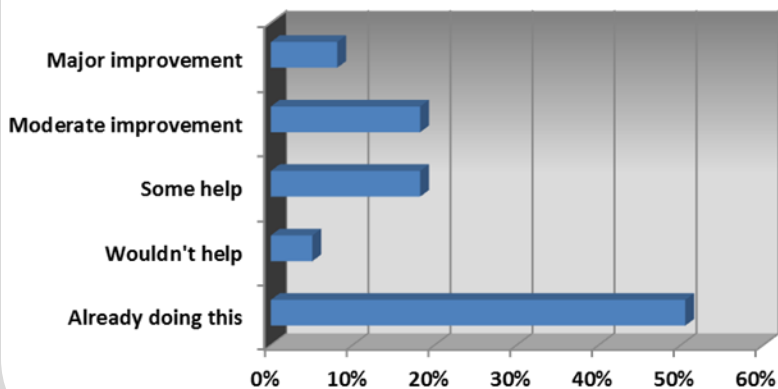
Only 18% of our respondents believe they would see major or moderate benefits from reducing the number of security products and vendors in their organizations.

A much larger number (73%) say that they've either already done this or that it wouldn't them help much. The idea that the incompatibilities and differences between security point products are causing a major amount of customer frustration isn't borne out in our results.
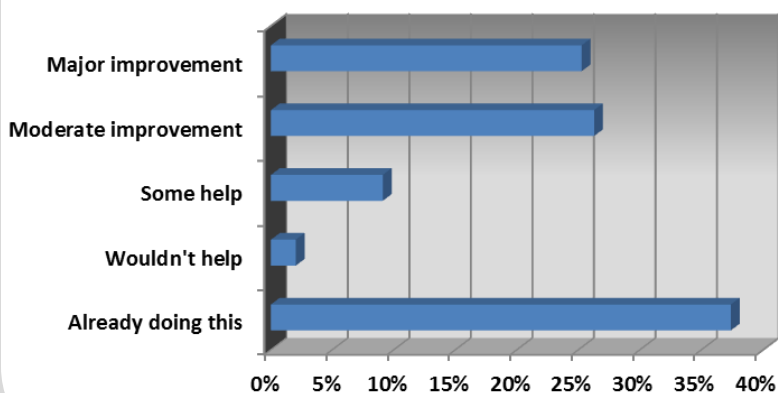
More clearly defined security standards & policies enterprise-wide

Category	
Major improvement	
Moderate improvement	
Some help	
Wouldn't help	
Already doing this	

0% 10% 20% 30% 40% 50% 60%

Just over half say that they already have clear security standards and policies, while 44% report that improving on this score would be of some help.

More than a quarter (26%) say that having more consistent policies and security standards clarified would be a major or moderate improvement to their overall security. As the number of ways that an organization can be attacked increases (via mobile, cloud, social networking, etc.) it's only going to become more difficult for them to respond with standards and policies that are not in step with the actual threats.
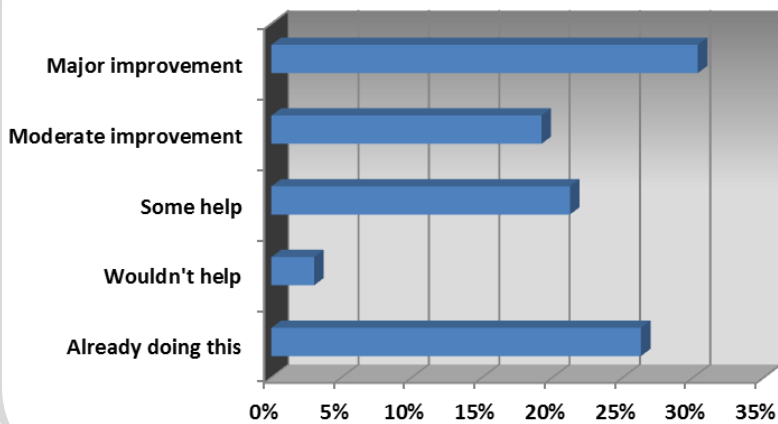
'Baking in' security from the beginning of each project - rather than bolting it on later

Category	
Major improvement	
Moderate improvement	
Some help	
Wouldn't help	
Already doing this	

0% 5% 10% 15% 20% 25% 30% 35% 40%

More than half say that security needs to be considered earlier and integrated more deeply into new IT projects. Only 37% say that they're already doing a good job on this; an additional 2% say that it wouldn't help.

Essentially, 60% of our respondents believe that their organizations fall short when it comes to ensuring that new IT initiatives take security considerations into account from beginning to end. This result will probably surprise managers of centralized security organizations, who likely believe that their departments are already ensuring that this happens.

Making security a higher priority organization-wide

Category	Value (approx.)
Major improvement	31%
Moderate improvement	20%
Some help	22%
Wouldn't help	4%
Already doing this	27%

(chart: bar graph with x-axis from 0% to 35%)

Not surprisingly, a large majority (70%) say that making security a higher priority would improve security to some degree. It's interesting to note that fully 30% believe that their organization would see a major improvement from a renewed focus on security, and an additional 19% say it would provide a moderate improvement.

On the positive side, it's good to see that a quarter of these orgs have already decided to concentrate more attention and resources on security.

The best way to improve data center security is to make sure that security is a key (and early) consideration in every IT project. According to our survey respondents, security isn't an early enough or deep enough part of new IT initiatives. They also say that overall data center security would be most improved by the organization making security a higher priority.

In qualitative responses, they related how management sometimes seems to view security as an annoying overhead expense – right up until they experience an attack or security breach – which "tends to focus their attention wonderfully," to quote one respondent.

Focused attention and consistent effort is what it will take to keep private data private in the future. While most organizations seem to be mostly on the right track (centralizing security, establishing standards, etc.) many of these efforts are still coming up short in terms of actual results. There's a lot of room for improvement when it comes to data center security – as daily headlines about breaches will attest.

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