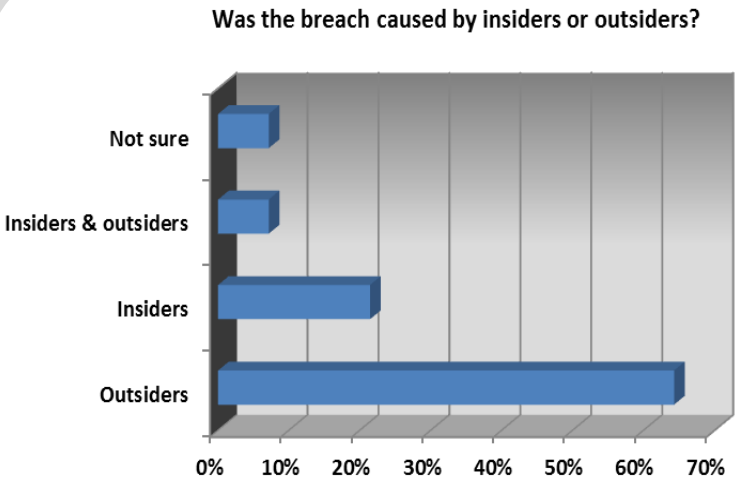
2011 Data Center Security Survey: Breaches – Impact & Remediation

Hardly a day goes by without a new story about some sort of IT security breach. The source of these security breaches can range from a confederation of politically motivated hackers intent on exposing confidential data to offshore professional criminals using automated bots to harvest personal data in order to defraud banks and consumers. Employees of a firm or its affiliated companies can also seek to steal or expose confidential data. The bottom line is that IT organizations today are perpetually under some sort of attack – whether it's by automated bots or bad guys targeting a specific company.

As part of our **2011 Data Center Security Survey**, we asked our data center respondents a set of questions about security breaches and their impact on both the business and IT sides of their organizations (survey demographics available here). Of our 147 respondents, around 20% said that their organization had experienced a breach (or breaches) in the last 18 months.

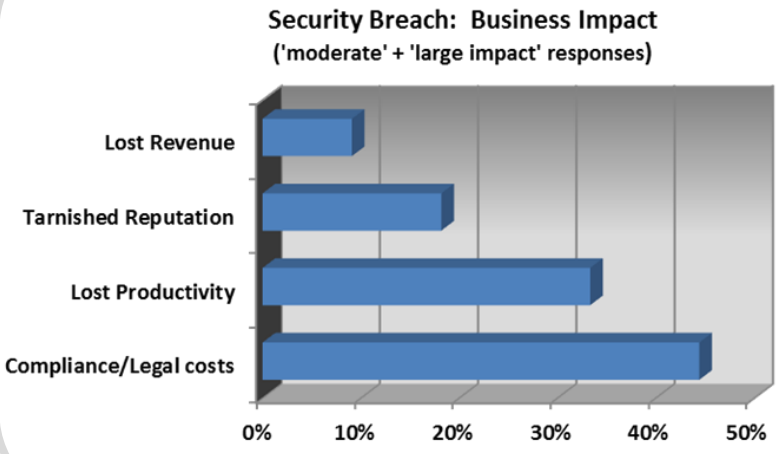
Customers answered all of the following questions in terms of the specific security incidents they experienced. Our first question asks whether an outside party or someone inside the organization caused the problem (or problems)…



While security experts say that 'insider risk' is more dangerous than the risks posed by outsiders, the breaches experienced by our respondents were mainly caused by outsiders.

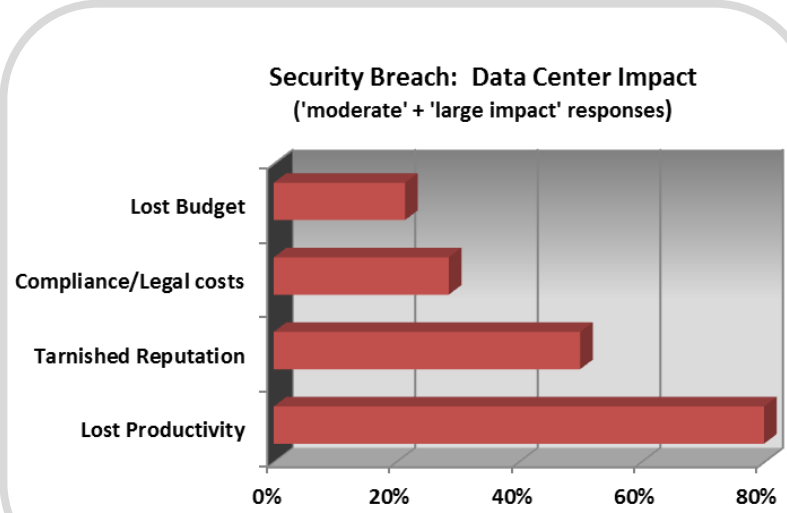
Even though insiders were responsible for only 20% of the breaches, the damage from these attacks can be far greater than what an outsider might cause. A burglar who has the keys to your house and car can steal a lot more of your possessions than one who has to break a window or pry open the front door.

In the next set of questions, we approach the cost of these security breaches from two different angles: we ask them to differentiate between the cost/damage to the overall business vs. the cost/damage to the data center organization. The differences between the two are interesting and highly informative…



On the business side of the organization, the biggest negative effect of the security breach was higher legal and compliance costs. But lost productivity, probably due to system downtime, was cited by a third of our respondents as having a 'moderate' or 'large impact' on the overall business.

Fewer cited lost revenue or a tarnished public reputation as a cost. This is perhaps because our respondent base didn't include anyone who has been involved in a highly public breach; it could also be due to respondents wishing to keep details confidential.

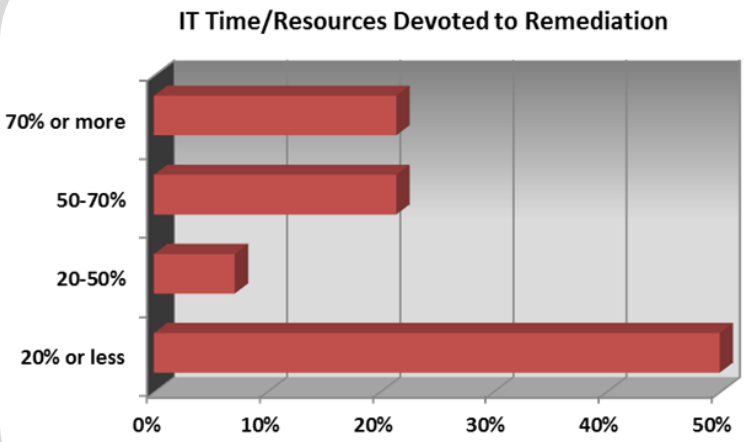


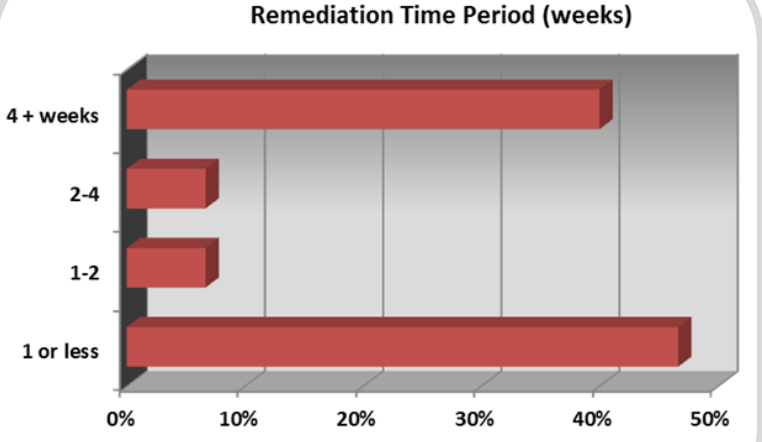
The impact of a security breach looks to be significantly more damaging to the data center than to the overall business. A huge majority, 80%, said that their breaches resulted in considerable lost productivity for the data center staff.

About half said that the breach tarnished the reputation of their IT shop. About a quarter reported that the breach resulted in higher legal and compliance costs – some of which were borne by the data center budget, we assume.

It's clear that the consequences from an IT security breakdown hit the data center harder than the non-IT part of the organization – at least that's what our survey respondents are reporting.

Next, we take a look at remediation time and costs….





These next two questions focus on the remediation process and its cost to the IT organization. For purposes of these questions, remediation was defined as everything from discovering the breach, assessing the damage, informing management and/or law enforcement, and fixing the problem.

Just over 40% of our respondents said that their breach remediation was an 'all hands on deck' effort requiring 50% or more of their IT staffing and other resources. For almost half (48%), the process of finding, assessing, and fixing the security problem required 20% or less of their IT resources.

We see a big split in terms of how long the remediation process lasted. Almost half reported that their efforts took one week or less. But just under 40% said that remediation took at least a month – or longer.

Obviously, security breaches aren't fun for anyone; they're typically painful and costly for all involved. For the data center, they are particularly painful because it's assumed that IT is a competent guardian of the organization's data assets. When a security breach occurs, it can cause the rest of the business to view the data center as weak, or lacking in expertise – which adds insult to injury.

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