Executive Summary: Corporate Security Organizational Structure, Cost of Services and Staffing Benchmark

---

A Security Leadership Research Institute Report

July 2011

INTRODUCTION

In the security industry large scale benchmarks are not easy to come by and one of the biggest hurdles is identifying what to measure. Each organization has their own culture, their own area of focus and their own idea of what is important which in turn drive the selection of metrics they will accept as a benchmark. Trying to come up with the one metric everyone accepts is a fool's errand. Consequently a practitioner is sometimes confronted with benchmark surveys that at the outset do not appear to match their specific needs, often resulting in non-participation.

This leads to a critical issue in our security and risk management community: A lack of readily available benchmark data to use to compare your organization risk management posture to others.

The objective of the Security Leadership Research Institute (SLRI) is to address this unmet need. The SLRI intends to be a resource for strategic security and risk management leaders seeking the key benchmarks that are relevant to their purpose.

We hope this executive summary will encourage more practitioners to participate in the SLRI. The only cost to you is the time to participate in our research studies and the return is access to the full results of which this executive summary only hints at. We are committed to build out a valuable source of knowledge for the security and risk management industry and we need your support to accomplish this goal.

This executive summary contains less than half of the valuable analysis that is available in the full report. For more information about the SLRI and to learn how to obtain the next edition of the full benchmark report see:
https://www.securityexecutivecouncil.com/about/research_institute.html

ABOUT THIS RESEARCH

The data used in this analysis comes largely from members of the SLRI and partially from the Tier 1 Security Leader™ community of the Security Executive Council. All participants are risk management practitioners comprising a broad cross section of industries. The organizations represented come from public and private sectors, and range from small and medium sized businesses to some of the largest international corporations.

Results, when possible, are broken down into categories so that you may select the appropriate metrics for your comparison purposes. The SLRI will only provide these categorized details when we have enough data to consider the results typical for the category or group and when we can ensure the anonymity of the participants and their organizations.
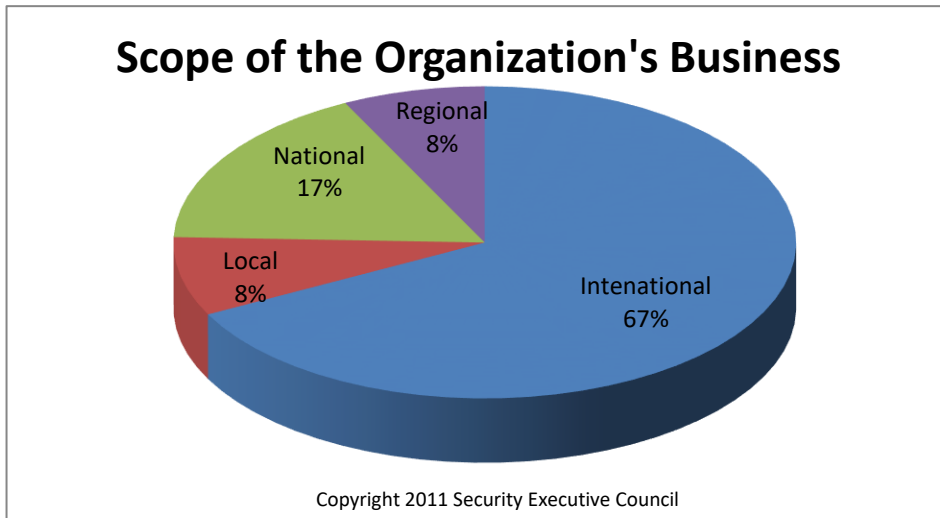
Over 180 organizations participated in this research. Not all questions were answered by all participants. We only included data when it was appropriate to do so and have made every attempt at preserving the quality of the reported results. Our sole purpose is to provide meaningful and useful information to you.

We intend to regularly update the results as we gain more participants in SLRI. We will continue to collect data with additions and refinements as suggested by our constituents for as long as the SLRI is a viable entity.
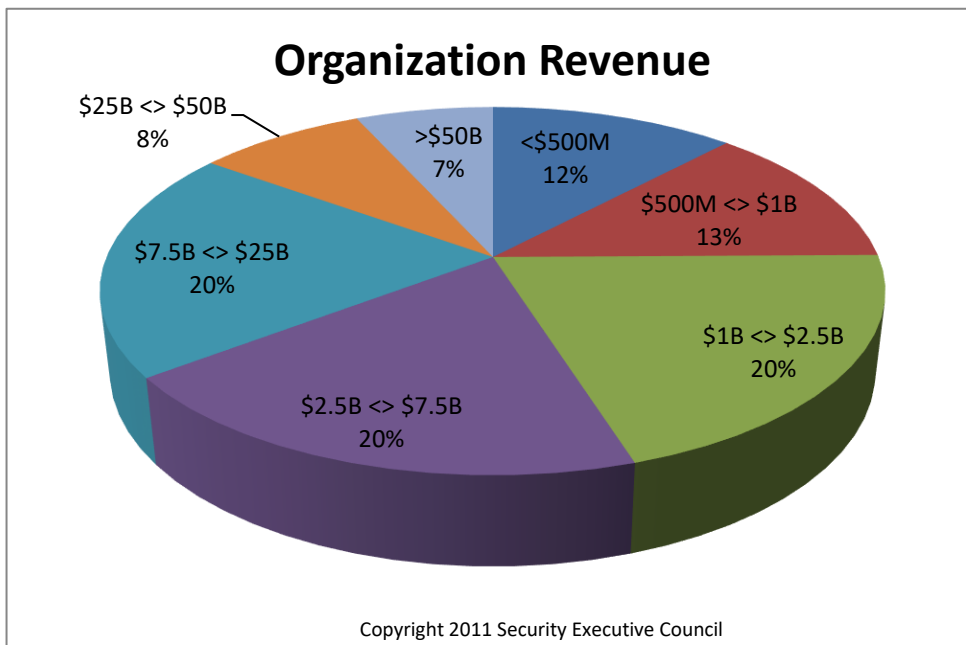
Demographics

The participants in this survey represented a broad array of business sizes and industries. More than half of the participating organizations operated outside the boundaries of the United States.

67% of respondents represented international organizations.

Scope of the Organization's Business

- Regional 8%
- National 17%
- Local 8%
- Intenational 67%
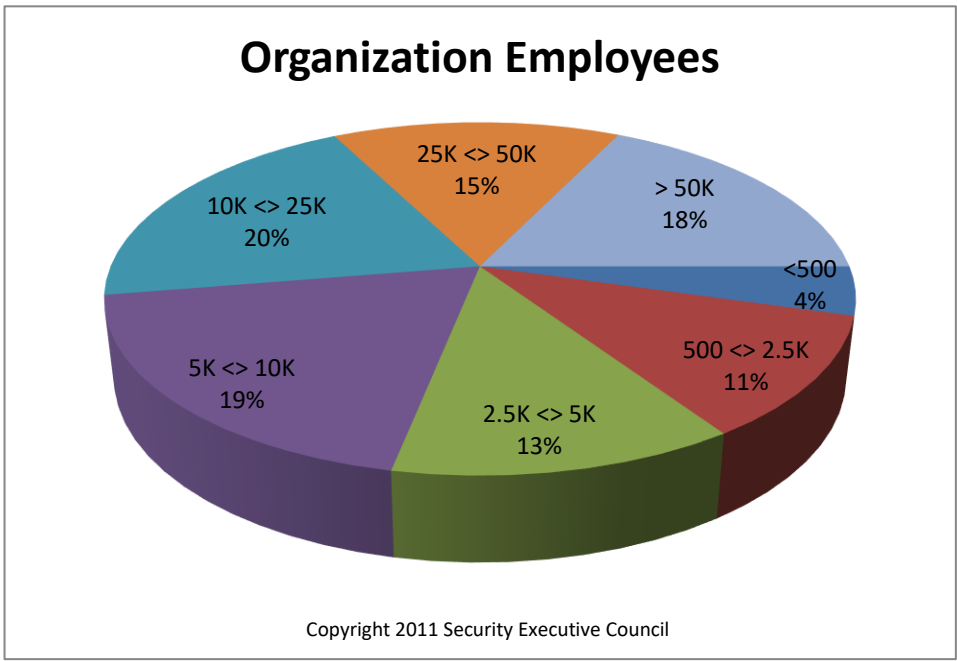
Copyright 2011 Security Executive Council

Note that the original survey question defined "Regional" in this question as "regional within a nation."
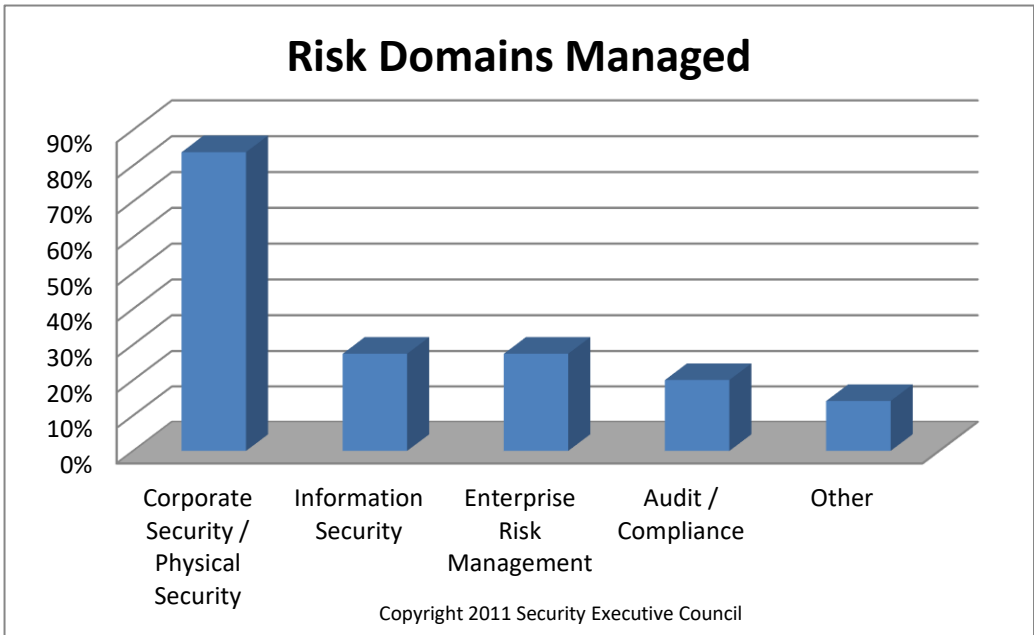
A large number of industries were represented in this research. The SLRI can provide industry specific benchmarks to specific industry groups given sufficient participation. If you are interested in seeing a detailed report for your industry specific security association have your association representative contact the SLRI for details.

Organization Revenue

- $25B <> $50B 8%
- >$50B 7%
- <$500M 12%
- $500M <> $1B 13%
- $7.5B <> $25B 20%
- $1B <> $2.5B 20%
- $2.5B <> $7.5B 20%

Copyright 2011 Security Executive Council

Organization revenue was converted to U.S. Dollars when appropriate.

Organization Employees

25K <> 50K
15%

> 50K
18%

<500
4%

500 <> 2.5K
11%

2.5K <> 5K
13%

5K <> 10K
19%

10K <> 25K
20%

Copyright 2011 Security Executive Council

61% of respondents operated at director level or above.

Risk Domains Managed

Copyright 2011 Security Executive Council

Respondents were allowed to choose multiple responses to security areas managed. Further analysis showed that 53% of respondents managed only Corporate Security / Physical Security and 7% of respondents managed only Information Security. Sixteen percent of respondents had responsibility for both Corporate Security / Physical Security and Information Security.

73% of respondents report to vice-president level or above.

To get a better idea of the level in the organization the typical security and risk management executive operated at we asked two questions. The first question asked the respondent to select the title level that best represented who they reported into. Since organizational structures vary we also wanted to know how many reporting levels the respondent was away from the organization's senior-most operating executive.

61% of respondents are within two reporting levels of the senior-most operating executive.

Further analysis of the levels of reporting seemed to indicate that the size of the organization was not a determining factor in whether or not a security executive is likely to directly report to the senior most operating executive.

There was little commonality regarding which business area the security groups report into. There is no clear correlation between business area reported into and any attribute measured in this survey, this included organization industry, size (both revenue and employee count), scope of organization and scope of responsibility.
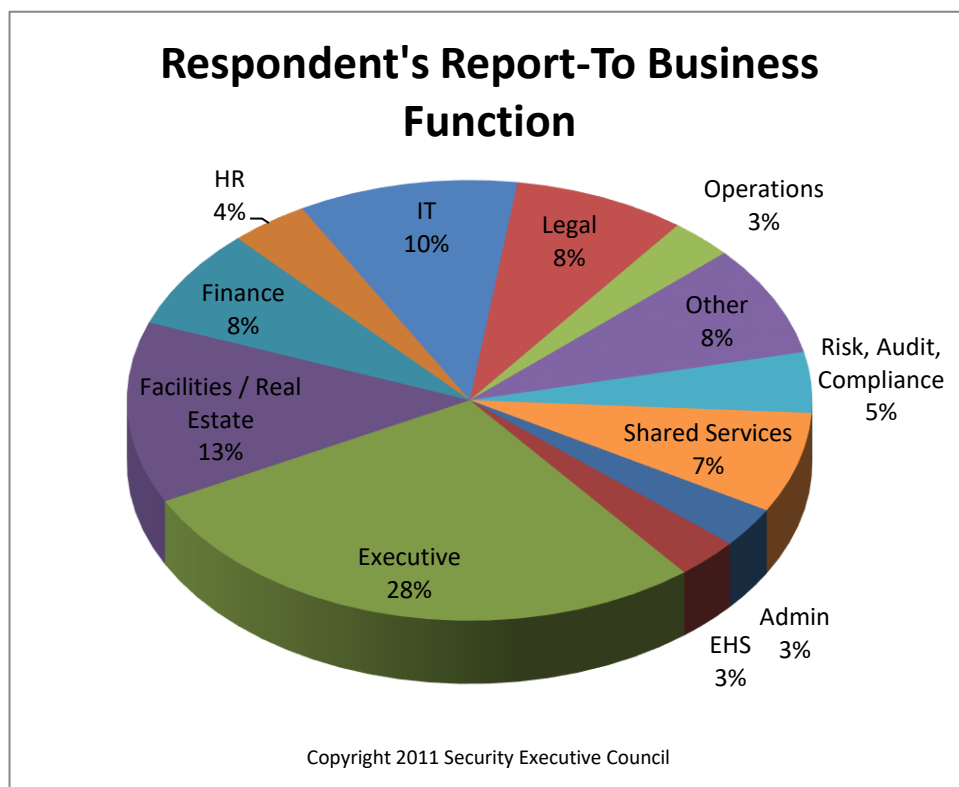
60% of respondents have a multi-national or global / international scope of responsibility

Security Budget

As each organization is different and characterizes the security budget in different ways we provide budget figures broken down across various different categories. Our goal is to provide risk management professionals a way to obtain a rough estimate of typical security budget size.

Overall the average security budget reported was $8 million.

The security budget figures provided by participants spanned a very wide range. Overall averages can only be used to get a rough understanding of security budgets. The full report (available only to those that participate in the SLRI) provides further detail such as security budget by size/revenue of the organization, operating scope, title level of the respondent and other criteria.

Overall the average security budget $ per organization employee was $249.

Overall the average security budget as a percentage of organization revenue was 0.07%.

Security Staffing

This research investigated typical security staffing. The full report delves into the detail by comparing staffing levels to a number of different criteria. A couple highlights are provided here:

On average respondents reported one security employee for every 99 organization employees.
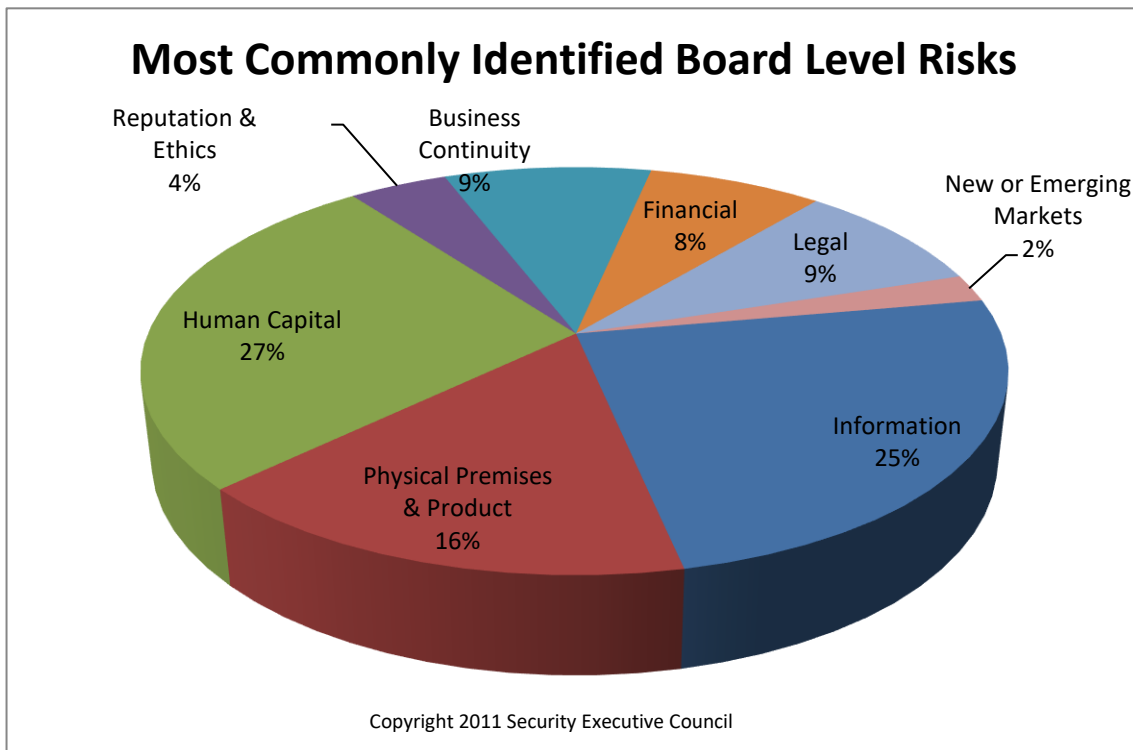
On average a typical respondent managed a staff made up of 85% uniformed security.

Risk breakdown by the Security Executive Council's Board Level Risk Categories

As discussed in the March 2010 issue of Corporate Secretary[1] "…a failure to recognize the potential consequences of risk failure can bring serious damage to companies." Security and risk management leaders must be able to effectively communicate Security's role in mitigating board level risk concerns to the board and executive management team.

Respondents were allowed to enter up to five risks that were the greatest concern to their organization. Responses were then categorized based on their best fitting Board Level Risk category (see Appendix A). The charts below can be used to identify the Board Level Risk categories that were most commonly chosen as high risks by the respondents.

---

[1] See Managing Enterprise-Wide Board Risk: https://www.securityexecutivecouncil.com/spotlight/?sid=25915&sc=SLRIrpt

Most Commonly Identified Board Level Risks

Reputation & Ethics 4%
Business Continuity 9%
Financial 8%
Legal 9%
New or Emerging Markets 2%
Human Capital 27%
Information 25%
Physical Premises & Product 16%

Copyright 2011 Security Executive Council

An astute reader may find value in the analysis of board level risk frequency broken down by other factors. That detail is provided in the full report that is only available to those who participate in the SLRI.

Program Drivers

Organizations have different key motivators for their risk management programs. Even within a particular organization different security programs may have different drivers depending on what risks they are addressing. While one type of driver is not necessarily better than another it is interesting to note which drivers are more prevalent than others.

The most common drivers for security programs were regulations, corporate culture and incidents.

Security Program Governance and Oversight

Respondents were allowed to select multiple ways their security program is governed. They also reported on the type of corporate risk oversight team that existed within their organization.

The most common method of governance for security programs was corporate policy followed closely by regulations and laws.

43% of organizations report either no risk oversight group exists or that security is not represented into the risk oversight group

Security Programs

Respondents were asked to provide the level of responsibility they had for selected programs or services at their organization. The available options were:

- Accountable
- Responsible
- Accountable and responsible
- Outside scope (meaning the program or service existed within their organization but the respondent was neither accountable nor responsible for it)
- Program does not exist

The following table shows the percentage of respondents that selected a particular level of responsibility for the given program or service. The full report (available to participants in the SLRI) shows the levels of responsibility given various criteria such as organization size and reporting structure.

Program	Most Common
Asset Protection, loss prevention	BOTH (64%)
Aviation security and operations	NONE (45%)
Awareness and education	BOTH (57%)
Brand, reputation, trademark/trade name	SCOPE (39%)
Business continuity/resiliency	SCOPE (32%)
Business ethics and compliance	SCOPE (47%)
Business intelligence and analysis	SCOPE (56%)
Emergency response and disaster recovery	BOTH (46%)
Guard service	NONE (81%)
Incident reporting	BOTH (70%)
Information security, application security	SCOPE (53%)
Information security, intellectual property protection	SCOPE (44%)
Information security, intrusion detection	SCOPE (56%)

Information security, systems and specifications: hardware	SCOPE (61%)
Information security, systems and specifications: software	SCOPE (61%)
Investigations (e.g. theft, fraud, threats, due diligence, conflict of interest)	BOTH (57%)
IT forensic investigation	SCOPE (54%)
Law enforcement liaison	BOTH (71%)
New product and marketing security	SCOPE (40%)
Personnel protection/work place violence	BOTH (56%)
Personnel screening, background investigations and due diligence	SCOPE (42%)
Physical site security design and system specifications	BOTH (66%)
Product protection (e.g. tampering, counterfeiting, diversion)	SCOPE (42%)
R&D security	NONE (31%)
Risk assessments	BOTH (62%)
Security related regulations and compliance management	BOTH (77%)
Security/business command center	BOTH (55%)
Supply chain security	SCOPE (31%)
Travel security	BOTH (40%)
Others:	NONE (85%)

APPENDIX A

Board Level Risk Categories

For more on what this chart represents and why it is important see "Managing Enterprise-Wide Board Risk":
https://www.securityexecutivecouncil.com/spotlight/?sid=25915&sc=SLRIrpt

About the Security Leadership Research Institute

The Security Leadership Research Institute (SLRI) is dedicated to providing independent and actionable research to the security and risk community. The SLRI was formed as a result of the need by the security industry to document the entire spectrum of risk mitigation and security through research. If you need to benchmark your programs, you need to become involved. There is no cost to join except a small amount of your time. Learn more here: www.securityexecutivecouncil.com/about/research_institute.html

About the Security Executive Council

The Council provides strategy, insight and resources to risk mitigation decision makers. Taking input from all industry segments the Council incorporates it into proven practices to provide an array of options that solve pressing issues. With a staff of more than 100 successful experienced security executives we work one-on-one with Tier 1 Security Leaders™ to help them reduce risk and add to corporate profitability in the process.

Contact:
To learn more about Council offerings and services: contact@secleader.com or fill out our information inquiry form available at: www.securityexecutivecouncil.com