Research Report

Abstract:

The Visibility and Control Requirements of Cloud Application Security

The Role of Cloud Access Security Brokers in Securing SaaS Applications and Other Cloud Security Considerations

By Doug Cahill, Senior Analyst; Jon Oltsik, Senior Principal Analyst; and Bill Lundell, Director of Research
With Jennifer Gahm, Senior Project Manager

May 2016

Introduction

Research Objectives

ESG's cloud security research was designed to gain insights into the awareness of, requirements for, and future plans with regard to cloud security. Participating organizations were required to be using cloud services in production, with individual respondents responsible for or highly familiar with their company's cloud security requirements, challenges, and subsequent plans.

The survey was designed to answer the following questions:

- How do IT and security professionals compare the security (i.e., policies, processes, technologies, and skills) associated with on-premises IT infrastructure and applications against that of public cloud-based infrastructure/applications?
- What are the top security concerns related to organizations' use of cloud services, including software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS)? What areas of cloud security do organizations believe require the most improvement?
- What technologies do organizations use for enforcing cloud security policies?
- What factors are considered when assessing the security risks associated with a cloud application?
- What is the impact of the unauthorized use of cloud services, i.e., shadow IT, on securing corporate data assets?
- How is compliance with industry regulations affected by the use of cloud services?
- Are organizations prepared to secure their use of cloud services with respect to policies, methodologies, skills, tools, and funding?
- Are organizations using cloud access security broker (CASB) solutions to control the use of cloud applications?
- What was or will be the initial CASB use cases for current and potential users of these solutions?
- What is the relative effectiveness of existing security technologies?
- What is the prioritization of functional and architectural requirements for cloud security solutions?
- From what type of security vendor do IT decision makers expect to source cloud security solutions?
- What are the organizational dynamics regarding new constituents in cloud computing, i.e., application development and DevOps?
- What are organizations' future plans with respect to cloud security spending and skill set development priorities?

Survey participants represented a wide range of industries including manufacturing, financial services, health care, communications and media, retail, government, and business services. For more details, please see the Research Methodology and Respondent Demographics sections of this report.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey with IT/information security professionals responsible for/familiar with their organization's virtualized/cloud infrastructure ecosystem, especially the security requirements, challenges, and subsequent strategies, in North America (United States and Canada) between December 16, 2015 and January 18, 2016. To qualify for this survey, respondent organizations had to be using cloud computing infrastructure (i.e., private cloud or public cloud) as part of their IT production environment. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 302 IT/security professionals.

Please see the Respondent Demographics section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

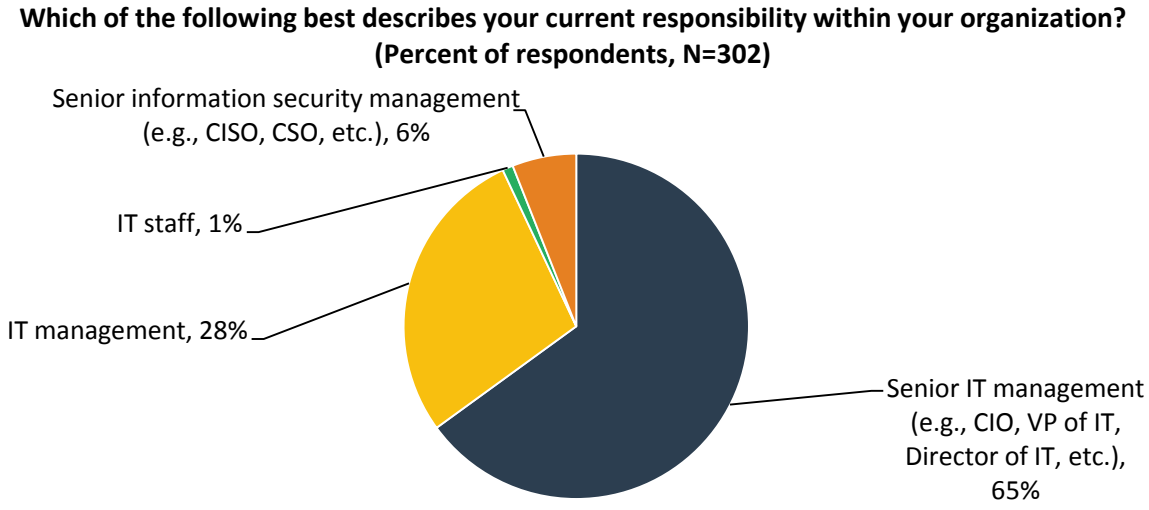
Respondent Demographics

The data presented in this report is based on a survey of 302 qualified respondents. Figures 1-4 detail the demographics of the respondent base, including individual respondents' current responsibilities, as well as respondent organizations' total numbers of employees, primary industries, and annual revenues.

Respondents by Current Responsibility

Respondents' current responsibilities are shown in Figure 1.

Figure 1. Respondents' Current Responsibility

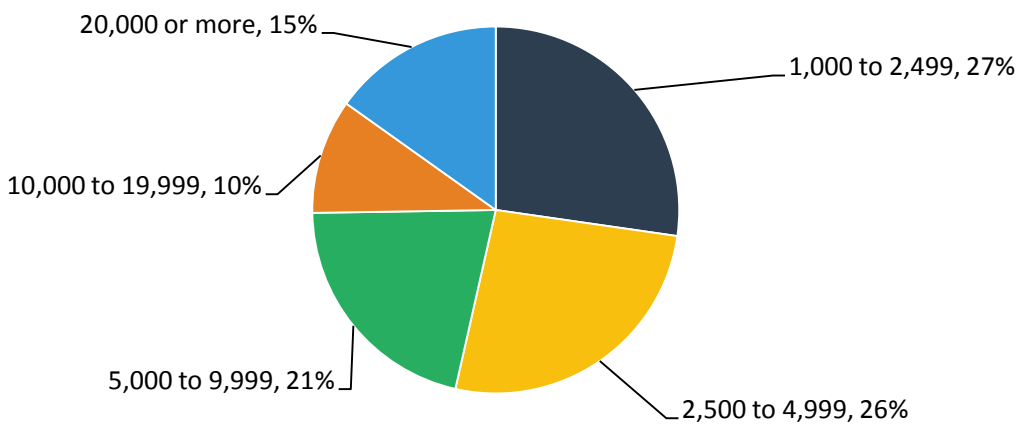


Source: Enterprise Strategy Group, 2016

Respondents by Total Number of Employees Worldwide

The number of employees in respondents' organizations is shown in Figure 2.

Figure 2. Respondents by Total Number of Employees Worldwide

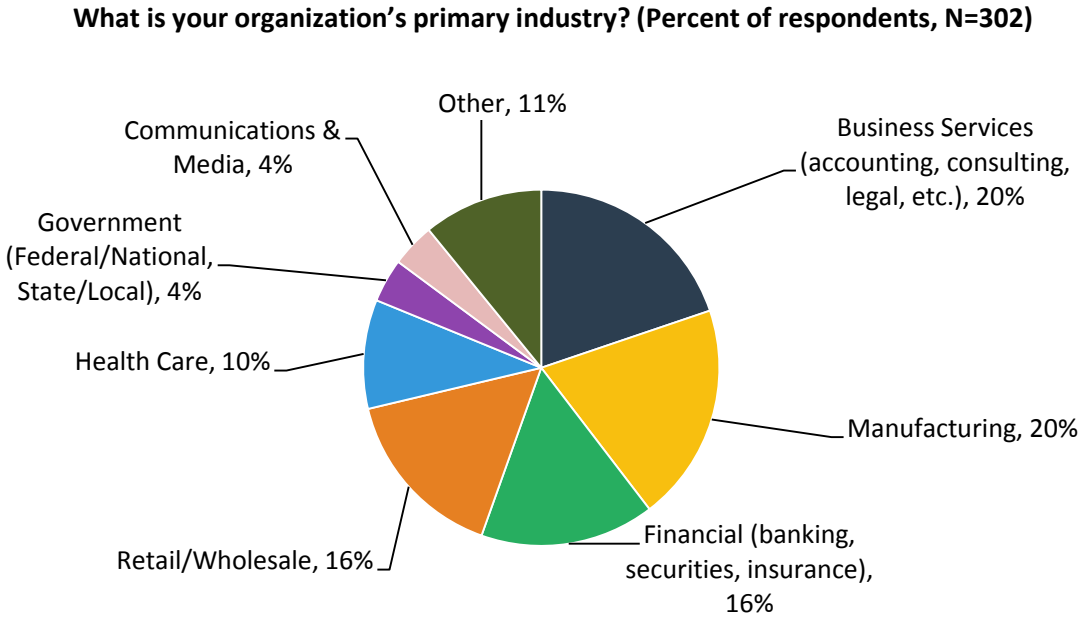


Source: Enterprise Strategy Group, 2016

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified respondents from individuals in 19 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 3.

Figure 3. Respondents by Industry

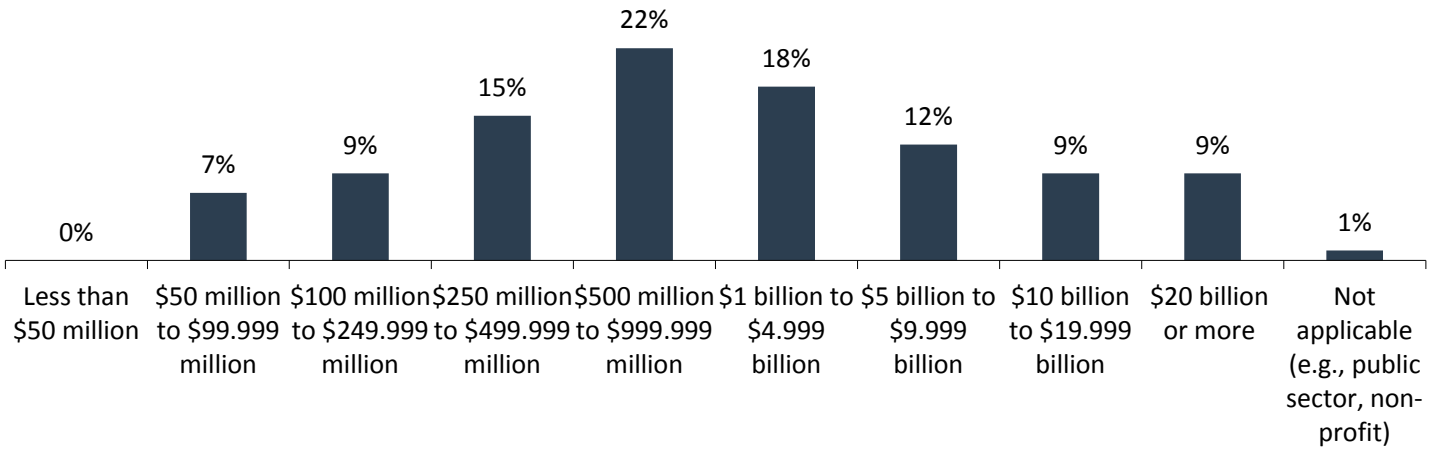


Source: Enterprise Strategy Group, 2016

Respondents by Annual Revenue

Respondent organizations' annual revenues are shown in Figure 4.

Figure 4. Respondents by Annual Revenue



Source: Enterprise Strategy Group, 2016

Contents

List of Figures

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188