Research Report

Abstract:

Cyber Supply Chain Security Revisited

By Jon Oltsik, Senior Principal Analyst

With Bill Lundell, Senior Research Analyst and Jennifer Gahm, Senior Project Manager

September 2015

Introduction

Research Objectives

In order to explore cyber supply chain security practices and challenges further, ESG surveyed 303 IT and information security professionals representing large midmarket (500 to 999 employees) organizations and enterprise-class (1,000 employees or more) organizations in the United States within vertical industries designated as critical infrastructure by the U.S. Department of Homeland Security (DHS). All respondents were familiar with/responsible for their organization's information security policies and procedures, especially with respect to the procurement of IT products and services. Respondents also had to be familiar with cyber supply chain security as defined previously.

The survey was designed to answer the following questions:

1. Risk management
   - Has the organization experienced any security breaches? If so, what was the impact?
   - How would respondents rate the security threat landscape now compared with two years ago? Do respondents expect the threat landscape to get worse over the next two years?
   - How well prepared is the organization for the current threat landscape?
   - Is executive management supporting and investing in cybersecurity?
2. Procurement
   - How important are IT vendors' security processes in customers' procurement decisions?
   - Do critical infrastructure organizations audit the development processes of vendors before purchasing IT products? If so, is there a common model for these audits? Are these standard activities and processes across the enterprise?
   - Are vendor cybersecurity audits a critical component of IT procurement or do purchasing managers have the discretion to purchase from IT vendors with sub-par product and process security?
3. Software development
   - Do critical infrastructure organizations include security considerations as part of their standard software development processes?
   - Have organizations experienced any security breaches related to internally developed software vulnerability?
   - Do critical infrastructure organizations require their internal developers to be trained in secure software development?
   - When organizations outsource their software development, are secure development processes a requirement for external outsourcers and contractors?
4. External IT security
   - To what extent do critical infrastructure organizations currently open their IT systems to external parties such as customers, suppliers, and business partners?
   - To what extent do critical infrastructure organizations currently consume IT services and applications provided by external parties such as customers, suppliers, and business partners?
   - How are these relationships secured? Are there formal processes and safeguards in place?
5. The role of the U.S. Federal Government

- Do cybersecurity professionals working at critical infrastructure organizations understand the U.S. government's cybersecurity strategy?
- Do critical infrastructure organizations believe that the Federal Government should do more or less in terms of cybersecurity defenses and strategies?
- What if any specific actions should the Federal Government take?

Survey participants represented industries designated as critical infrastructure by the U.S. Department of Homeland Security (DHS). These industries include agriculture and food, banking and finance, communications, defense industrial base, energy (utilities, oil, and gas), transportation systems, water supply, health care, etc. 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 of IT and information security professionals from private- and public-sector industries designated by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR) in the United States between February 2, 2015 and February 11, 2015. To qualify for this survey, respondents were required to be familiar with/responsible for their organization's information security policies and procedures, especially with respect to the procurement of IT products and services. Respondents also had to be familiar with the cyber supply chain risk management model. 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 303 IT and information 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

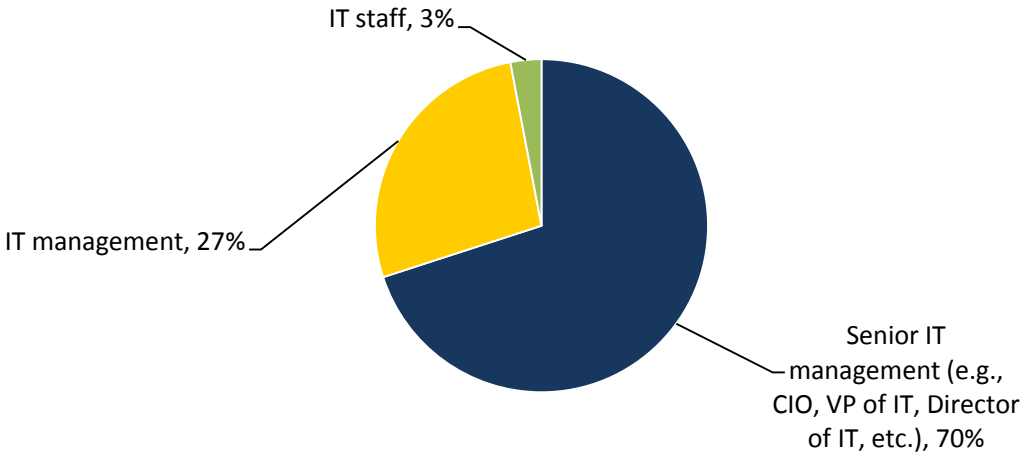
The data presented in this report is based on a survey of 303 qualified respondents. Figures 34-37 detail the demographics of the respondent base, including individual respondents' current job function, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Respondents by Current Job Function

Respondents' current job functions within their organizations is shown in Figure 1.

Figure 1. Survey Respondents by Current Job Function

Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=303)



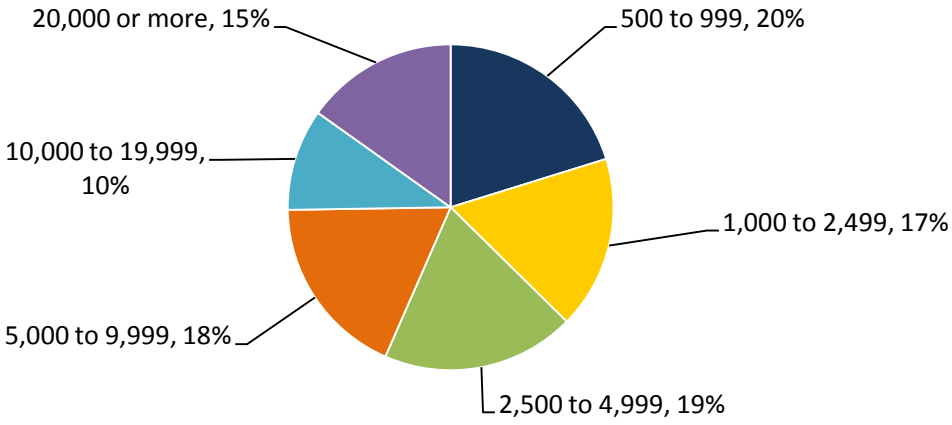
Source: Enterprise Strategy Group, 2015.

Respondents by Number of Employees

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

Figure 2. Survey Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of employees, N=303)

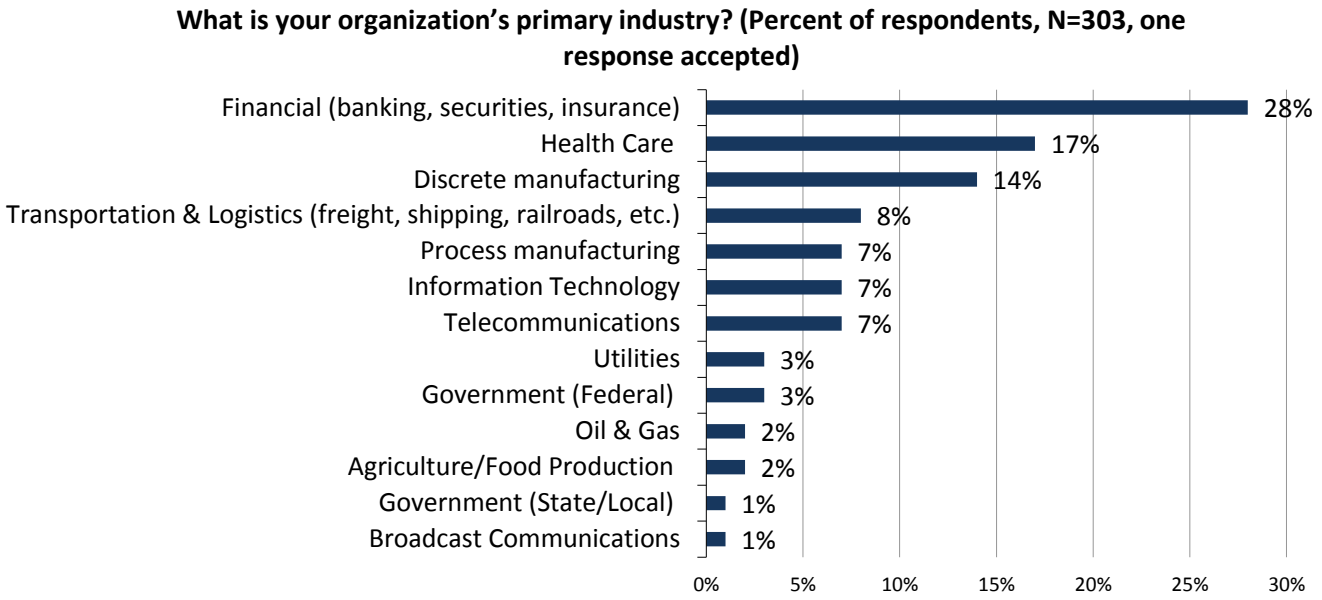


Source: Enterprise Strategy Group, 2015.

Respondents by Industry

Respondents were asked to identify their organization's primary industry. All respondent organizations were required to be part of industries categorized by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR), as shown in shown in Figure 3.

Figure 3. Survey Respondents by Industry

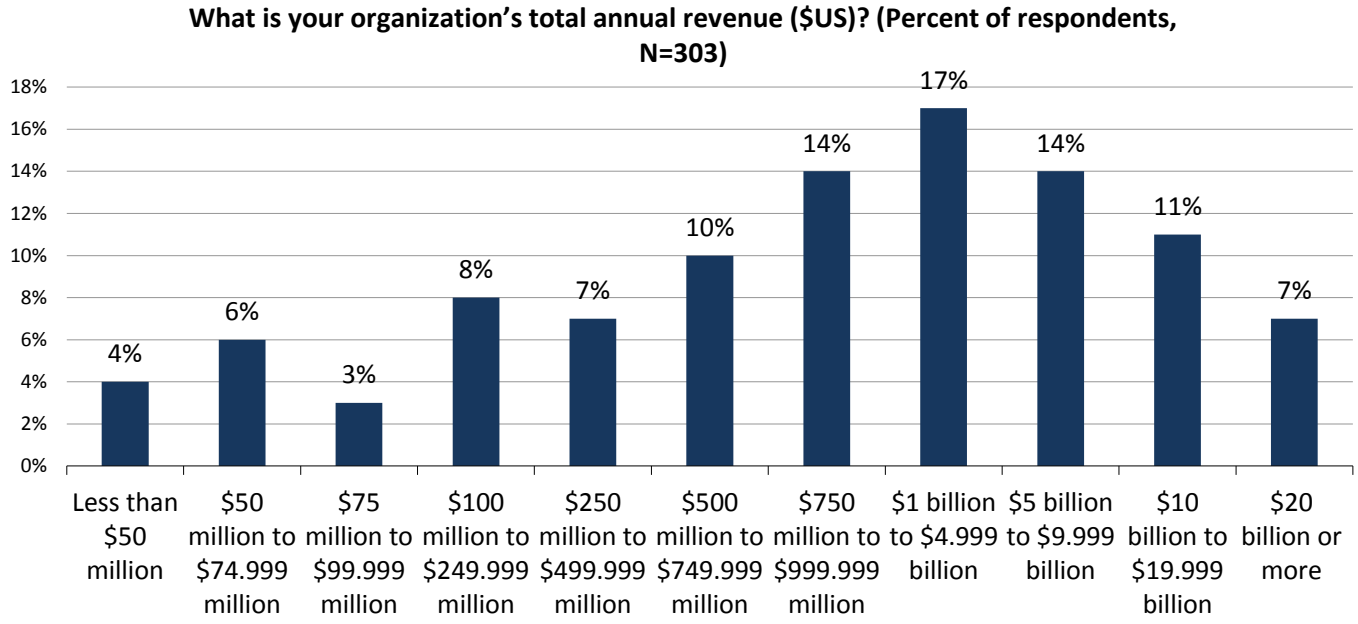


Source: Enterprise Strategy Group, 2015.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 4.

Figure 4. Survey Respondents by Annual Revenue



Source: Enterprise Strategy Group, 2015.

Contents

List of Figures

List of Tables

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0128 | www.esg-global.com