

Research Report

Abstract:

Threat Intelligence and Its Role Within Enterprise Cybersecurity Practices

*By Jon Oltsik, Senior Principal Analyst
With Bill Lundell, Senior Research Analyst and Jennifer Gahm, Senior Project
Manager*

June 2015

Introduction

Research Objectives

In order to assess how enterprise organizations are collecting, processing, analyzing, and operationalizing their threat intelligence programs, ESG surveyed 304 IT and information security professionals representing enterprise-class (1,000 employees or more) organizations in North America. All respondents were involved in the planning, implementation, and/or daily operations of their organization's threat intelligence program, processes, or technologies.

The survey and overall research project were designed to answer the following questions about:

- Threat intelligence programs
 1. Do enterprise organizations have threat intelligence programs in place?
 2. If so, how are they structured and funded?
 3. How mature are these programs?
 4. What are the primary objectives for threat intelligence programs?
- Threat intelligence knowledge and opinions
 1. Do security professionals have adequate threat intelligence skills?
 2. If not, where are the knowledge gaps?
 3. What is driving threat intelligence program strategy?
 4. What are the biggest threat intelligence challenges for organizations?
- The organization(s) responsible for threat intelligence programs
 1. Which groups are responsible for threat intelligence programs today? Do multiple groups participate in these programs?
 2. Who reviews threat intelligence and for what purposes?
 3. What do organizations actually do with the threat intelligence they collect, process, and analyze?
- Endpoint security technologies
 1. What types of internal and external threat intelligence data are organizations collecting?
 2. How do they select external threat feeds and services?
 3. Is threat intelligence data integrated with other security and IT technologies?
 4. Are security professionals aware of threat intelligence standards? If so, are these standards important?
- Threat intelligence sharing
 1. Are organizations sharing threat intelligence today? If so, is this a regular or ad-hoc occurrence?
 2. Are organizations willing to share internally-derived threat intelligence with the US Government? If so, what types of programs and assurances would they want from Washington?

Survey participants represented a wide range of industries including financial services, manufacturing, business services, communications and media, and government. 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 organizations in North America (United States and Canada) between February 27, 2015 and March 10, 2015. To qualify for this survey, respondents were required to be IT professionals directly involved in the planning, implementation, and/or daily operations of their organization's threat intelligence program, processes, or technologies. Respondent organizations also needed to currently be using external threat intelligence as part of its threat intelligence program.

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 304 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.

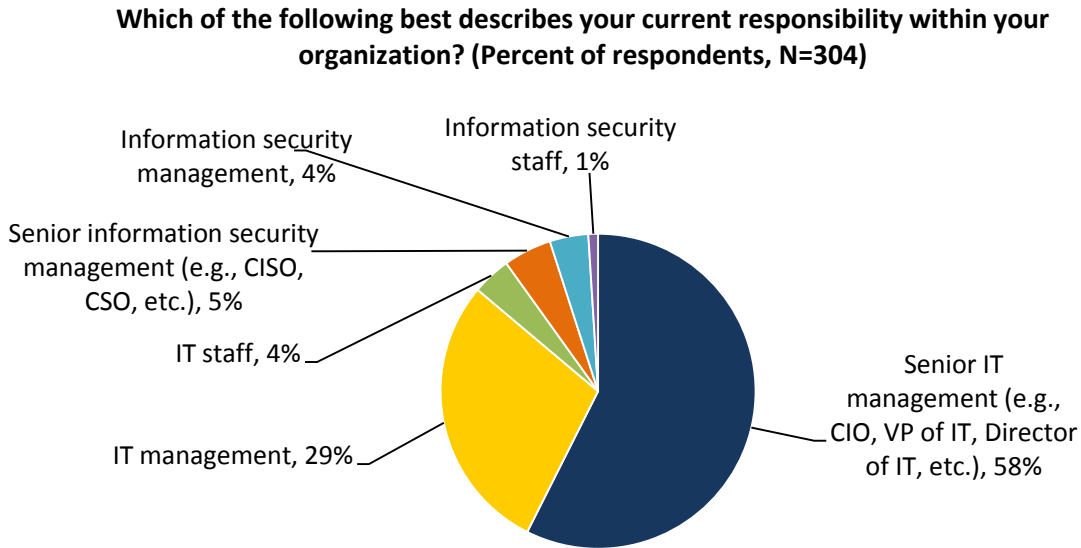
Respondent Demographics

The data presented in this report is based on a survey of 304 qualified respondents. The figures below detail the demographics of the respondent base, including individual respondents' current job functions, as well as respondent organizations' total numbers of employees, primary industries, and annual revenues.

Respondents by Current Job Function

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

Figure 1. Survey Respondents by Current Job Function

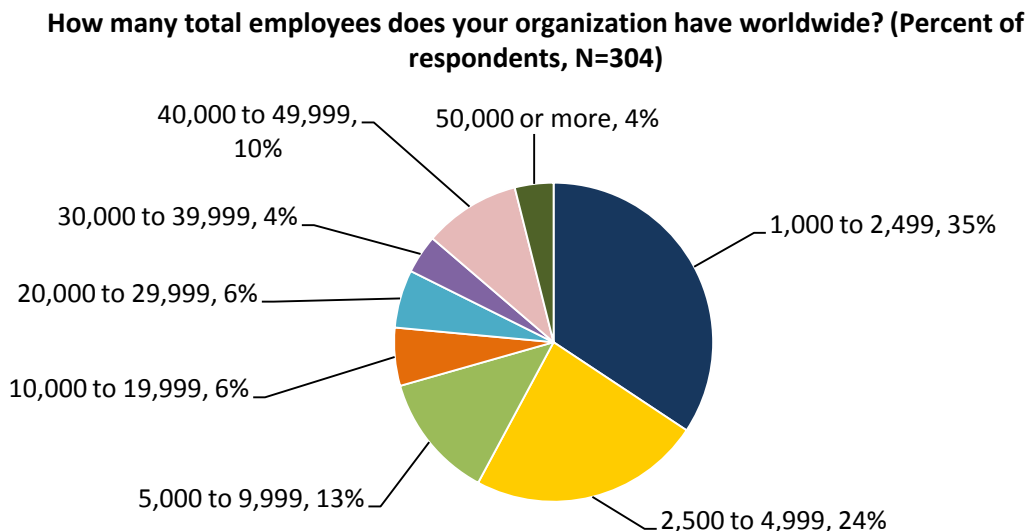


Source: Enterprise Strategy Group, 2015.

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

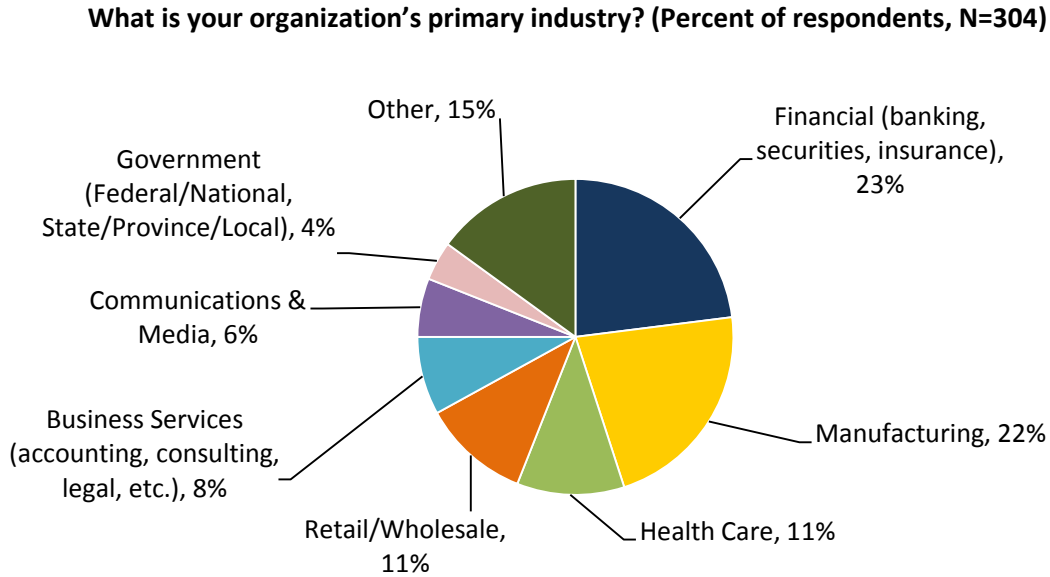


Source: Enterprise Strategy Group, 2015.

Respondents by Industry

Respondents were asked to identify their organizations' primary industry. In total, ESG received completed, qualified responses 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. Survey Respondents by Industry

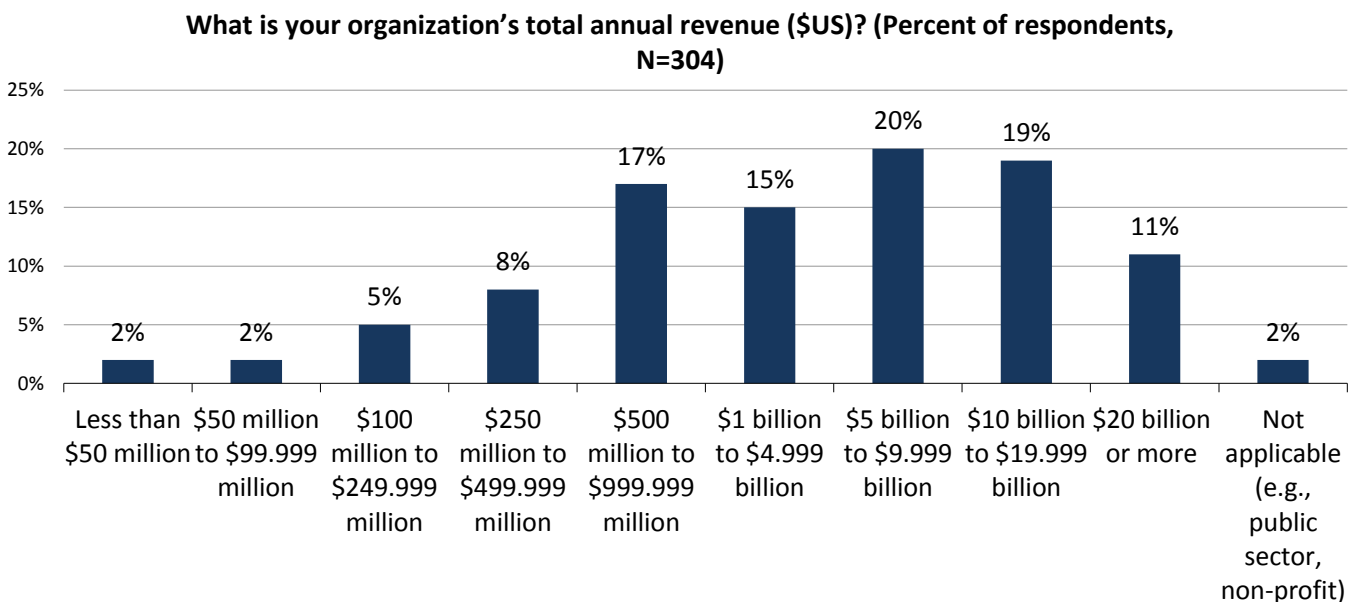


Source: Enterprise Strategy Group, 2015.

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	3
List of Tables	3
Executive Summary	4
Report Conclusions	4
Introduction	7
Research Objectives	7
Research Findings	8
Threat Intelligence Program Overview	8
Organizational Aspects of Threat Intelligence Program	12
Threat Intelligence Data Sources	17
Threat Intelligence Operations	24
Threat Intelligence Standards	27
Threat Intelligence Sharing	30
Future Threat Intelligence Strategy and Planning	35
Conclusion	38
Research Implications for Cybersecurity Professionals	38
Research Implications for Information Security Vendors	40
Research Implications for Governments	41
Research Methodology	43
Respondent Demographics	44
Respondents by Current Job Function	44
Respondents by Number of Employees	44
Respondents by Industry	45
Respondents by Annual Revenue	45

List of Figures

Figure 1. Length of Time Threat Intelligence Program Has Been in Place	8
Figure 2. Maturity Level of Organization’s Threat Intelligence Program	9
Figure 3. Reasons for Establishing a Threat Intelligence Program	10
Figure 4. Top Objectives of Organization’s Threat Intelligence Program	11
Figure 5. Individuals/Groups Most Responsible for Threat Intelligence Program	12
Figure 6. Number of Individuals that Review Threat Intelligence Daily	13
Figure 7. Staffing Level Dedicated to Threat Intelligence	13
Figure 8. How Threat Intelligence Program Is Funded	14
Figure 9. Respondents Rate Organization’s Threat Intelligence Skills	15
Figure 10. Metrics to Assess the Success of Threat Intelligence Program	16
Figure 11. Types of Internal Data Collected and Analyzed Today	17
Figure 12. Types of External Data Collected and Analyzed Today	18
Figure 13 Number of Different External Threat Intelligence Sources Used	19
Figure 14. Most Important Types of External Threat Intelligence Data	20
Figure 15. Criteria Used to Evaluate and Choose External Commercial Threat Intelligence Feeds/Services	21
Figure 16. Difficulty Determining Quality and Efficacy of Threat Intelligence Feeds	22
Figure 17. Redundancy of Commercial Threat Intelligence Feeds	23
Figure 18. Use of Threat Intelligence to Automate Prevention/Remediation Activities and Security Operations ..	24
Figure 19. Challenges Experienced with Collecting and Analyzing External Threat Intelligence	26
Figure 20. Familiarity with Threat Intelligence Standards	27
Figure 21. Importance of Threat Intelligence Standards	28
Figure 22. Use of Threat Intelligence Standards and Open Source Tools	29
Figure 23. Sharing of Internally-derived Threat Intelligence with Other Organizations/Industry ISACs	30
Figure 24. Value of Threat Intelligence Sharing Between Federal Agencies and Private Organizations	31
Figure 25. Willingness to Share Threat Intelligence with US Government Agencies	32
Figure 26. Filtering of Internally-derived Threat Intelligence Shared with Other Organizations/Industry ISACs	33
Figure 27. Actions US Government Would Need to Take to Make a Public/Private Threat Intelligence Sharing Program Valuable	34
Figure 28. Future Spending on Threat Intelligence	35
Figure 29. Organizations’ Plans for Internal and External Threat Intelligence	36
Figure 30. Actions Organizations Will Take to Support Their Threat Intelligence Programs	37
Figure 31. Survey Respondents by Current Job Function	44
Figure 32. Survey Respondents by Number of Employees	44
Figure 33. Survey Respondents by Industry	45
Figure 34. Survey Respondents by Annual Revenue	45

List of Tables

Table 1. Length of Time Threat Intelligence Program Has Been in Place, by Company Size	9
Table 2. Areas in Which Threat Intelligence Skills Are Fair or Poor, by Industry	16
Table 3. Difficulty Determining Quality and Efficacy of Threat Intelligence Feeds, by Industry	23
Table 4. Use of Threat Intelligence to Automate Prevention/Remediation Activities and Security Operations, by Industry	25
Table 5. Familiarity with Threat Intelligence Standards, by Company Size	28
Table 6. Importance of Threat Intelligence Standards, by Company Size	29
Table 7. Willingness to Share Threat Intelligence with US Government Agencies, by Company Size	32

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



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