Osterman Research
SURVEY REPORT

Survey Report by Osterman Research
Published **December 2019**

The Value of Threat Intelligence

Figures in this Report

Figure 1: Primary Industry Served by Respondent Organizations 3
Figure 2: "Which of the following best describes your organization's team focused on threat intelligence?" 4
Figure 3: Survey Respondents' Roles Within the Organization 5
Figure 4: Decision Makers' Concerns About Various Threats 6
Figure 5: Organizations' Current and Planned Use of Threat Intelligence, 2019 and 2020 6
Figure 6: Sources Used for Threat Intelligence 7
Figure 7: Challenges With Threat Intelligence 8
Figure 8: Interest in Threat Attribution for Targeted and Non-Targeted Attacks 9
Figure 9: Importance of Various Reasons to Perform Threat Attribution 9
Figure 10: Seriousness of Various Scenarios 10
Figure 11: "Does understanding the source of threats allow you to focus on the threats that matter to you?" 11
Figure 12: Extent to Which Decision Makers Agree Threat Attribution Allows Them to Prepare For and Respond to Threats 12
Figure 13: Extent to Which Employees in the Organization are Interested in Threat Attribution 12
Figure 14: Reasons That Organizations Would Share Information About Threat Attribution Outside of the Organization 13
Figure 15: Entities With Which Organizations Share Information About Targeted and Non-Targeted Attacks 13
Figure 16: Reasons That Organizations Would Choose Not to Report an Incident to Stakeholders 14
Figure 17: Perceived Utility of the MITRE ATT&CK Framework for Operationalizing Threat Intelligence, 2019 and 2020 15

Overview

Cyber security is an ongoing battle between sophisticated and well-funded bad actors and those who must defend corporate networks against their attacks. The bad news is that the latter are typically not winning. A recent Osterman Research survey[i] found that while most organizations self-report that they are doing "well" or "very well" against ransomware, other types of malware infections, and thwarting account takeovers because of the significant emphasis placed on these threats, they are not doing well against just about every other type of threat. These include protecting data sought by attackers, preventing users from reaching malicious sites after they respond to a phishing message, eliminating business email compromise (BEC) attacks, eliminating phishing attempts before they reach end users, and preventing infections on mobile devices.

This missing component for most organizations is the addition of robust and actionable threat intelligence to their existing security defenses, which can be segmented into four subcategories[ii]:

1. Strategic (non-technical information about an organization's threat landscape)
2. Tactical (details of threat actors' tactics, techniques and procedures)
3. Operational (actionable information about specific, incoming attacks)
4. Technical (technical threat indicators, e.g., malware hashes)

The use of good threat intelligence can enable security analysts, threat researchers and others to gain the upper hand in dealing with cyber criminals by giving them the information they need to better understand current and past attacks, and it can give them the tools they need to predict and thwart future attacks. Moreover, good threat intelligence can bolster existing security defenses like SIEMs and firewalls and make them more effective against attacks. Threat intelligence plays a key role in proactive defense to ensure that all security programs are relevant to the fast-evolving threat landscape. This is particularly valuable in security awareness training to ensure users are familiar with known threats.

ABOUT THIS WHITE PAPER

This survey report presents the results of a primary market research survey conducted with members of the Osterman Research survey panel and another panel and others during mid-2019. The survey was conducted with 227 individuals. To qualify for the survey:

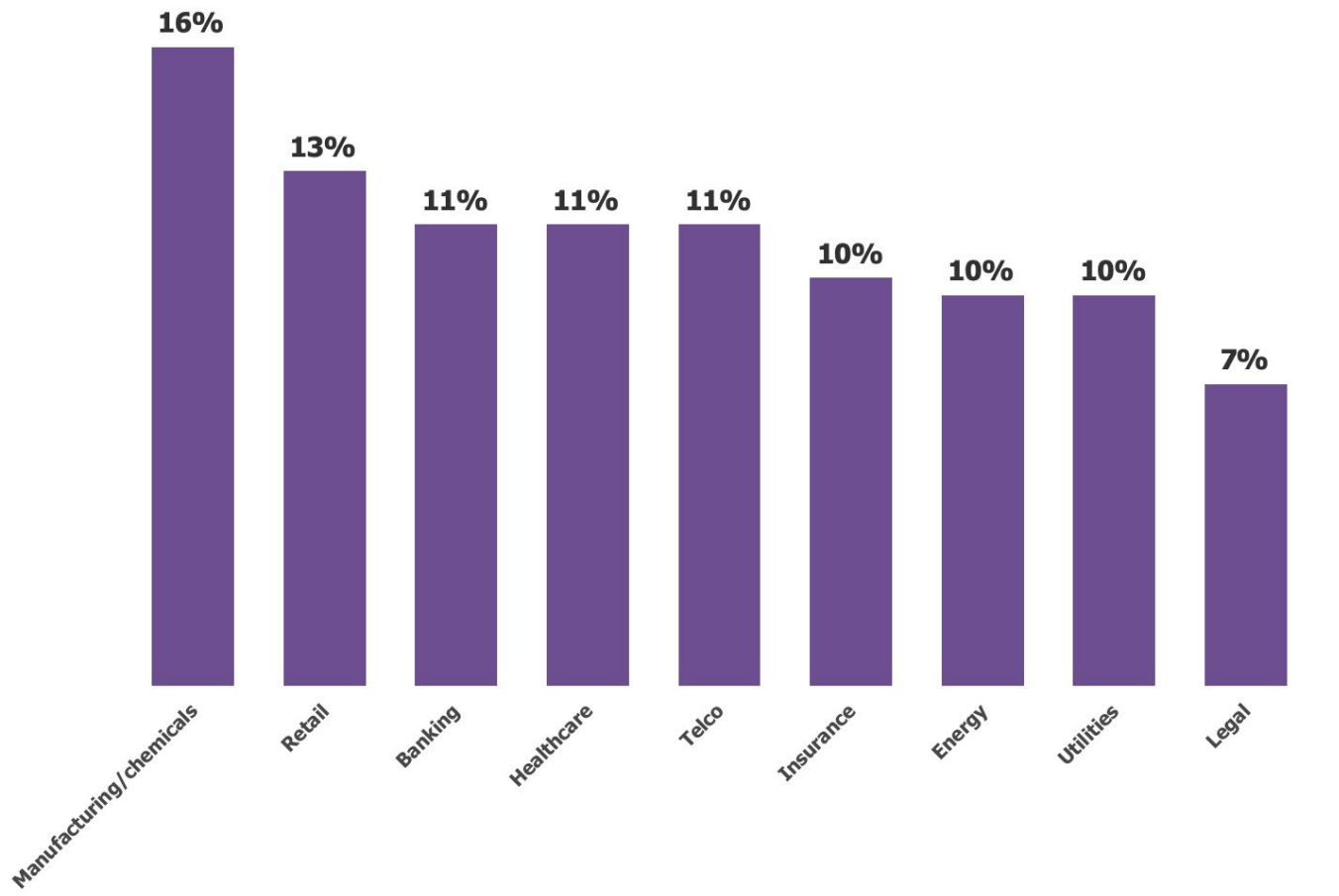
- Respondent organizations had to have at least 2,500 employees.
- Respondent organizations could not be a government entity.
- Respondents had to be involved in acquiring and/or using security in their organization.

Here are the key details of organizations' sizes:

- Mean number of employees at the organizations surveyed: 17,154 (median was 5,000).
- Mean number of email users at the organizations surveyed: 14,845 (median was 3,500).

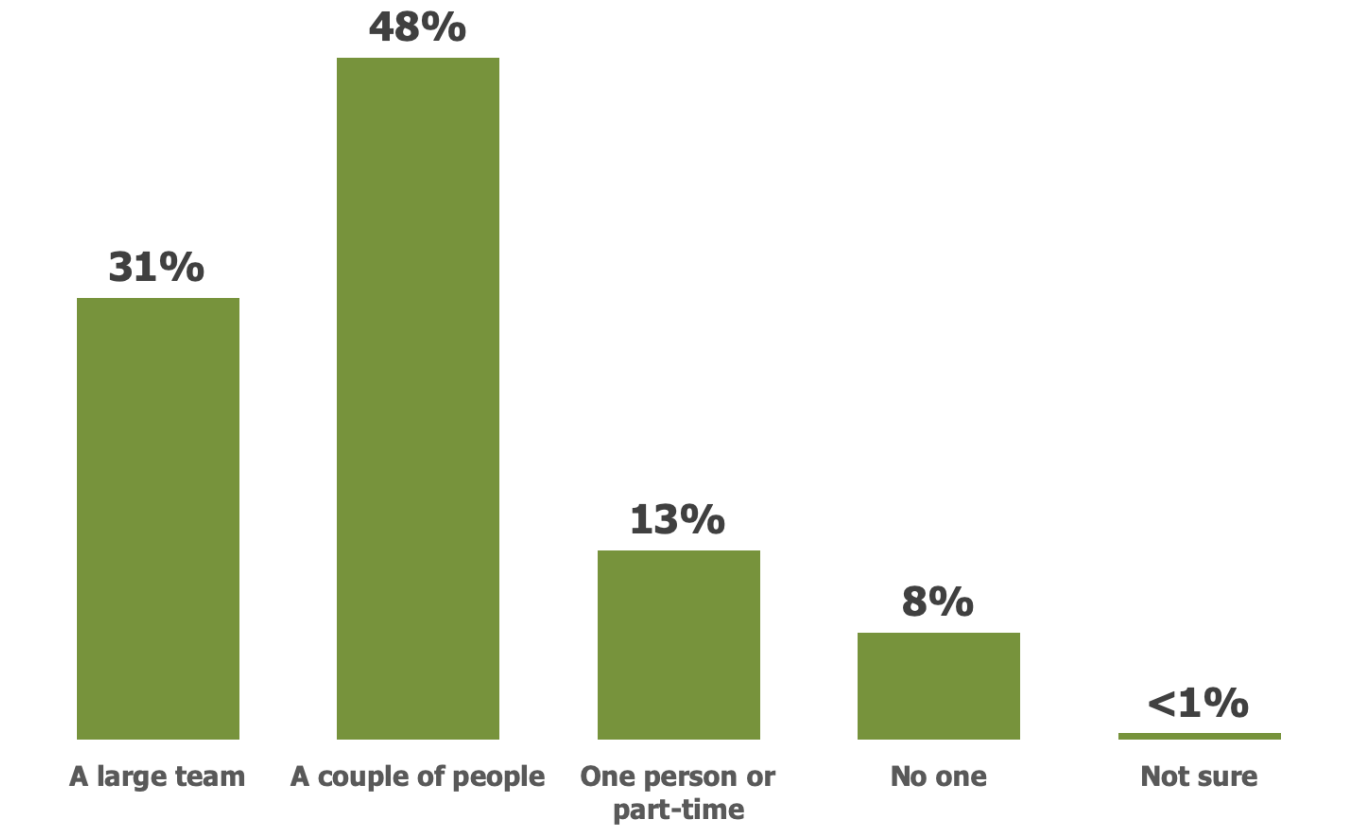
Survey Findings

Figure 1
Primary Industry Served by Respondent Organizations



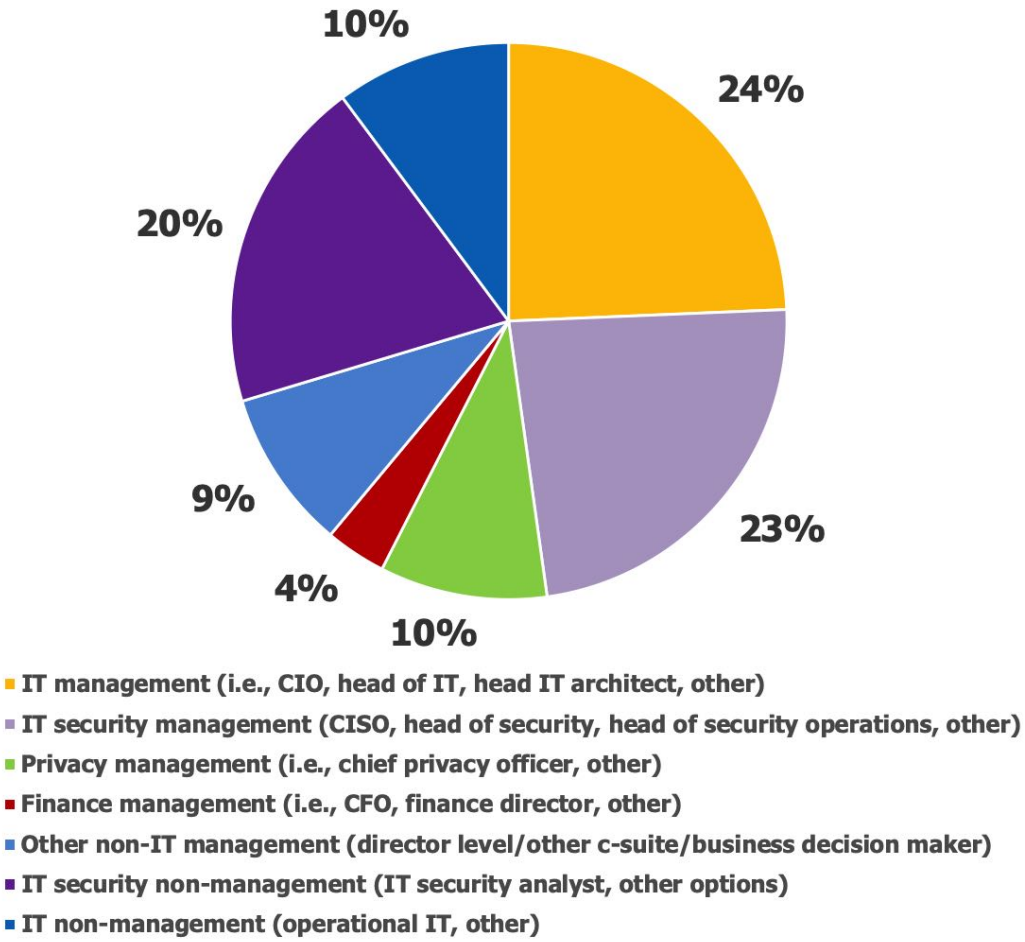
Source: Osterman Research, Inc.

Figure 2
"Which of the following best describes your organization's team focused on threat intelligence?"



Source: Osterman Research, Inc.

Figure 3
Survey Respondents' Roles Within the Organization



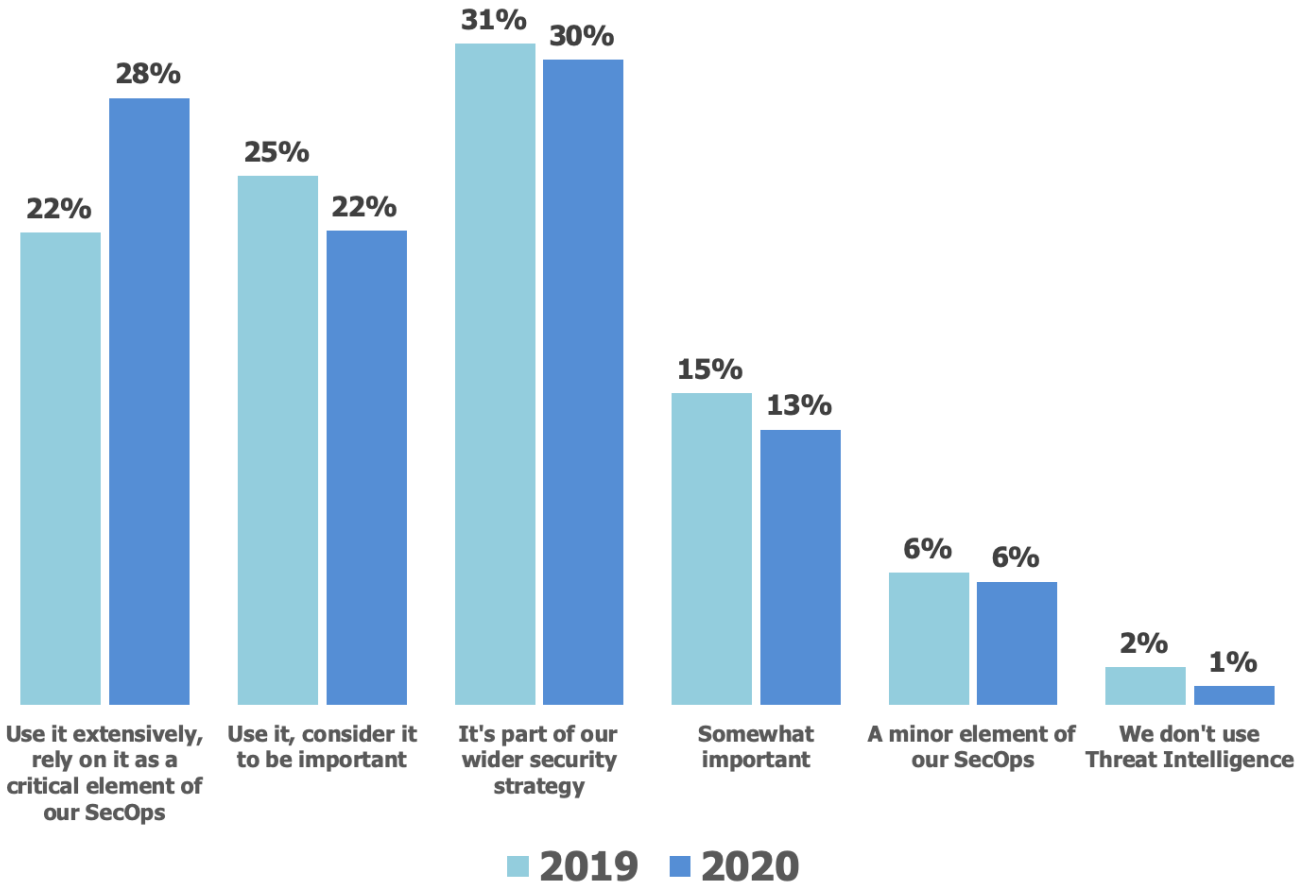
Source: Osterman Research, Inc.

Figure 4
Decision Makers' Concerns About Various Threats
Percentage responding "concerned" or "very concerned"

Threat	%
Malicious insiders stealing data	67%
Advanced persistent threats	62%
Malware infiltration (other than ransomware)	62%
Accidental data leakage	60%
Ransomware	59%
Violating regulatory obligations (e.g., GDPR, CCPA)	59%
Web surfing that could result in malware infiltration	53%
CEO Fraud/Business Email Compromise	52%
Spearphishing delivered through email	47%
Account takeovers	46%
Phishing delivered through email	44%
BYO device/cloud/mobile app problems	40%

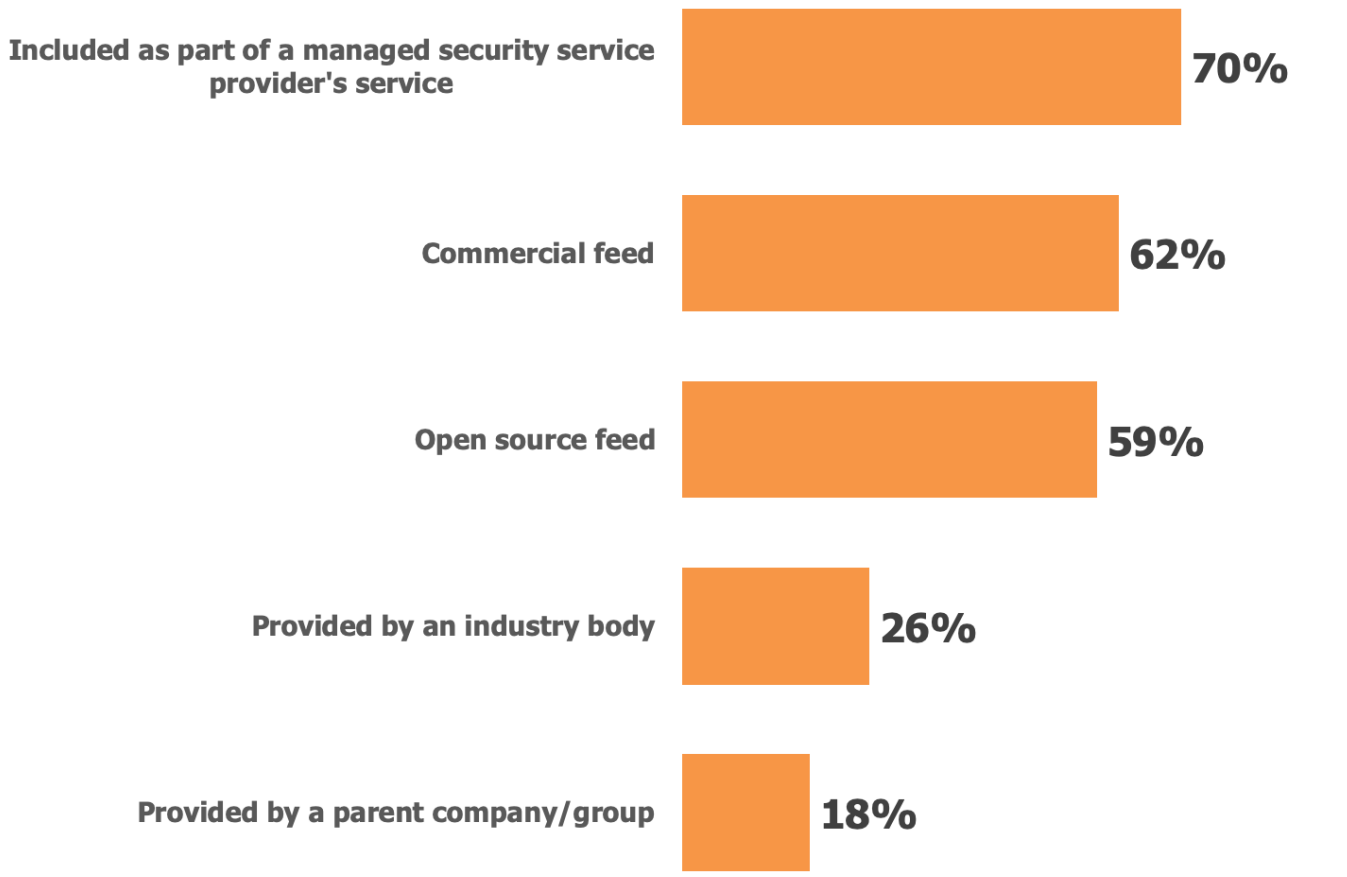
Source: Osterman Research, Inc.

Figure 5
Organizations' Current and Planned Use of Threat Intelligence, 2019 and 2020



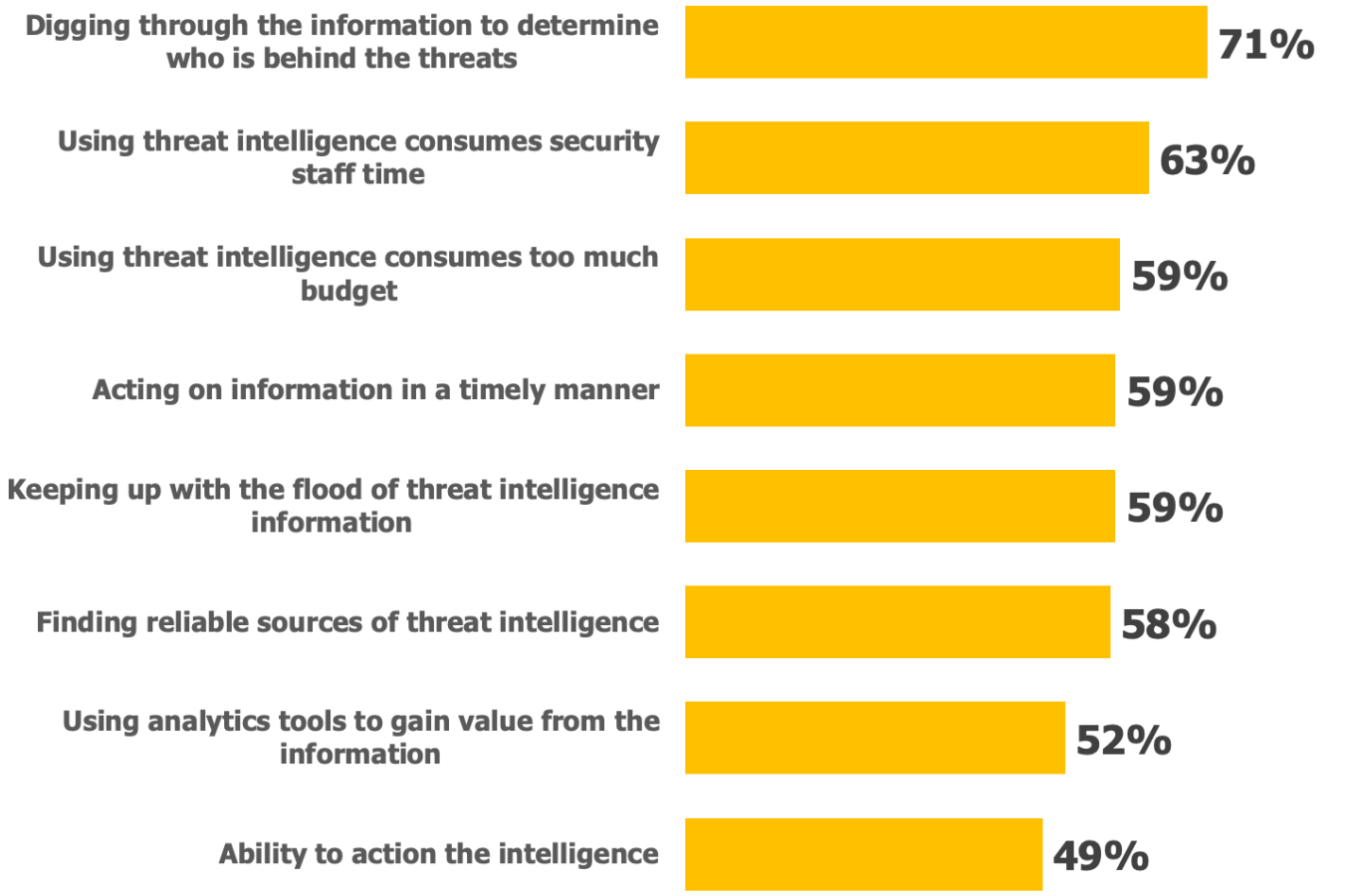
Source: Osterman Research, Inc.

Figure 6
Sources Used for Threat Intelligence
Percentage of organizations responding



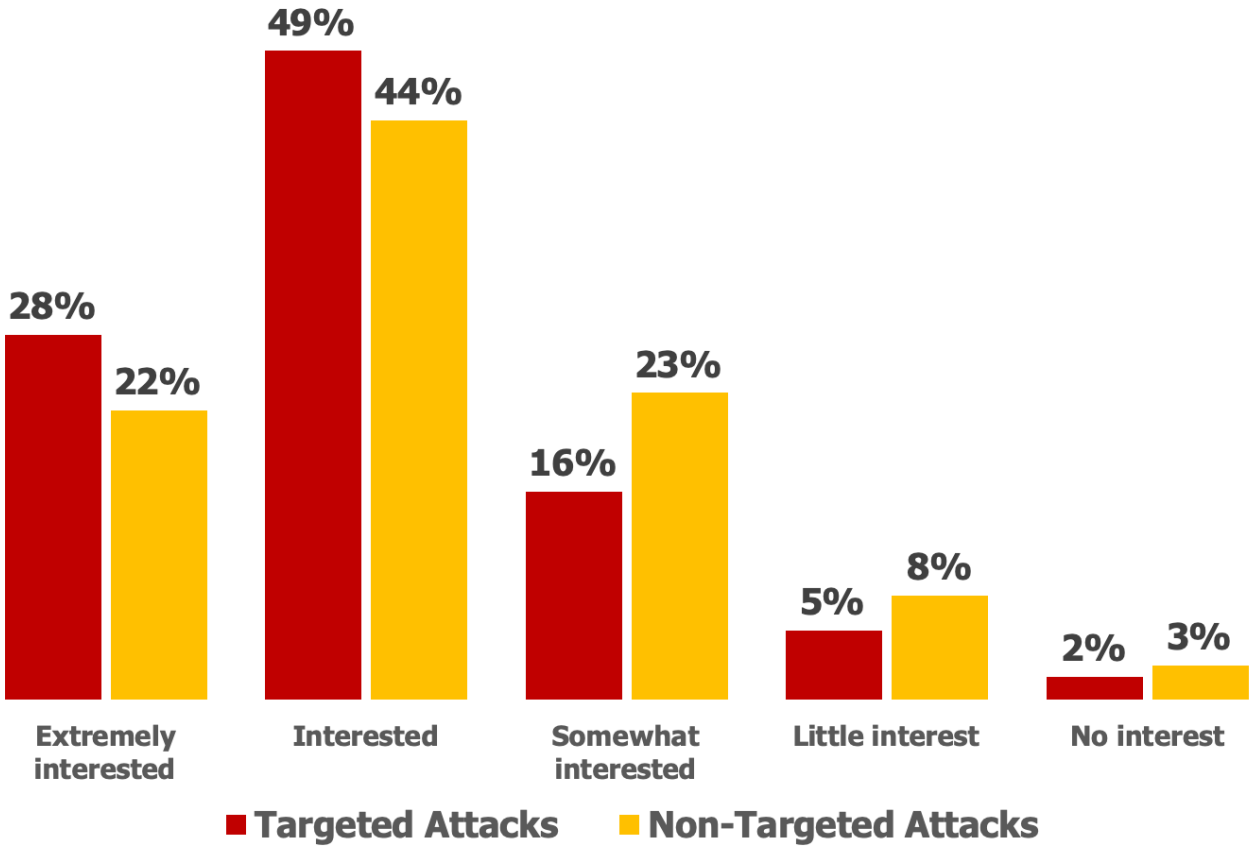
Source: Osterman Research, Inc.

Figure 7
Challenges With Threat Intelligence
Percentage responding a "significant" or "major" challenge



Source: Osterman Research, Inc.

Figure 8
Interest in Threat Attribution for Targeted and Non-Targeted Attacks



Source: Osterman Research, Inc.

Figure 9
Importance of Various Reasons to Perform Threat Attribution
Percentage responding "important" or "extremely" important

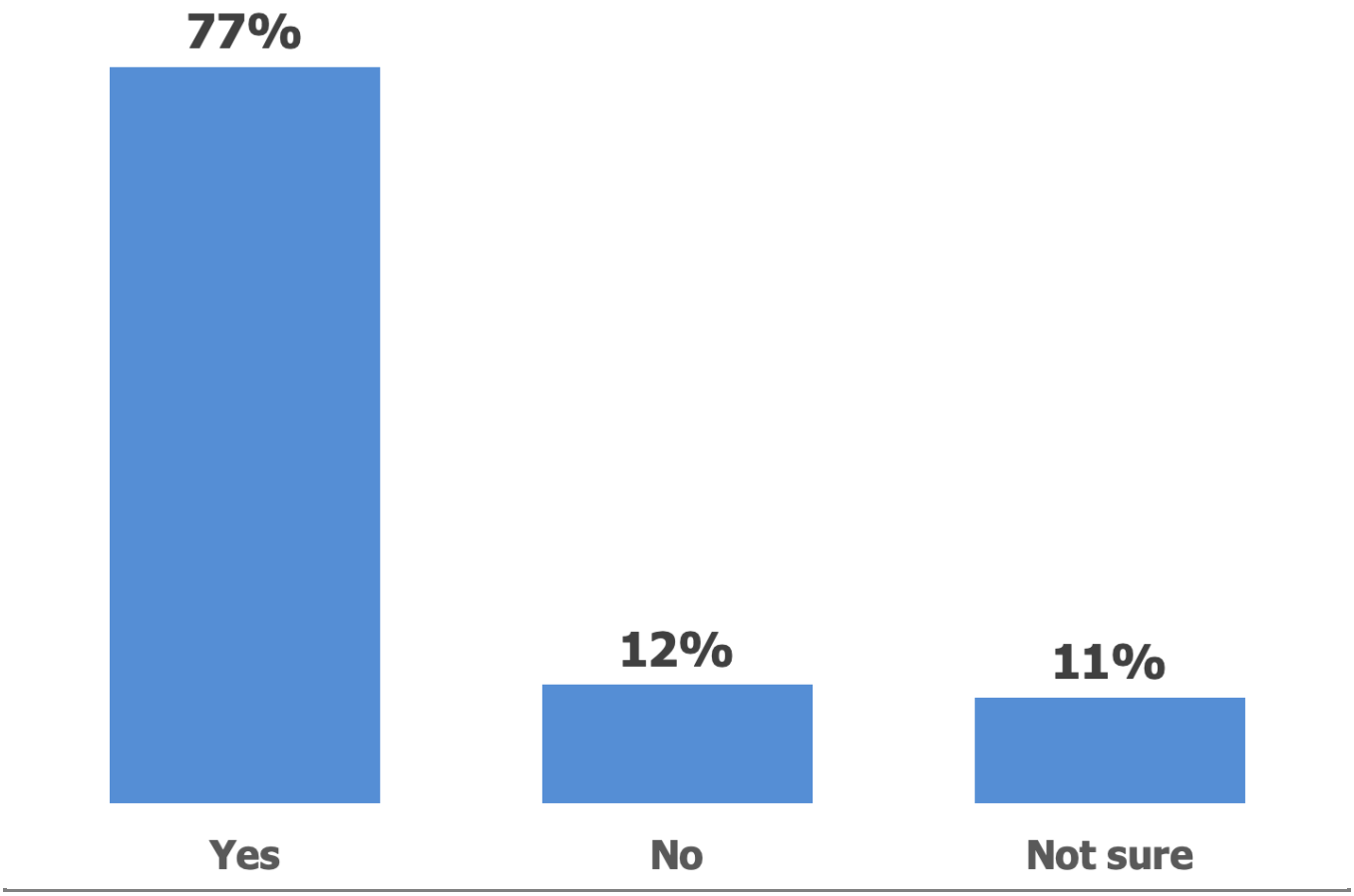
Reason	%
To respond to threats more quickly	89%
To prevent future threats more effectively	86%
To better understand existing vulnerabilities	83%
To improve our overall security strategy	79%
To know how to improve our security infrastructure	78%
To respond to threats more knowledgably	78%
To determine if our intellectual property was leaked and who is now in possession of it	74%
To know where to focus our security resources	73%
To give our security team confidence that they are focusing their efforts in the right places	71%
To better understand our adversaries	61%
To determine if nation-states are behind attacks	59%

Source: Osterman Research, Inc.

Figure 10
Seriousness of Various Scenarios
Percentage responding "serious" or "very serious"

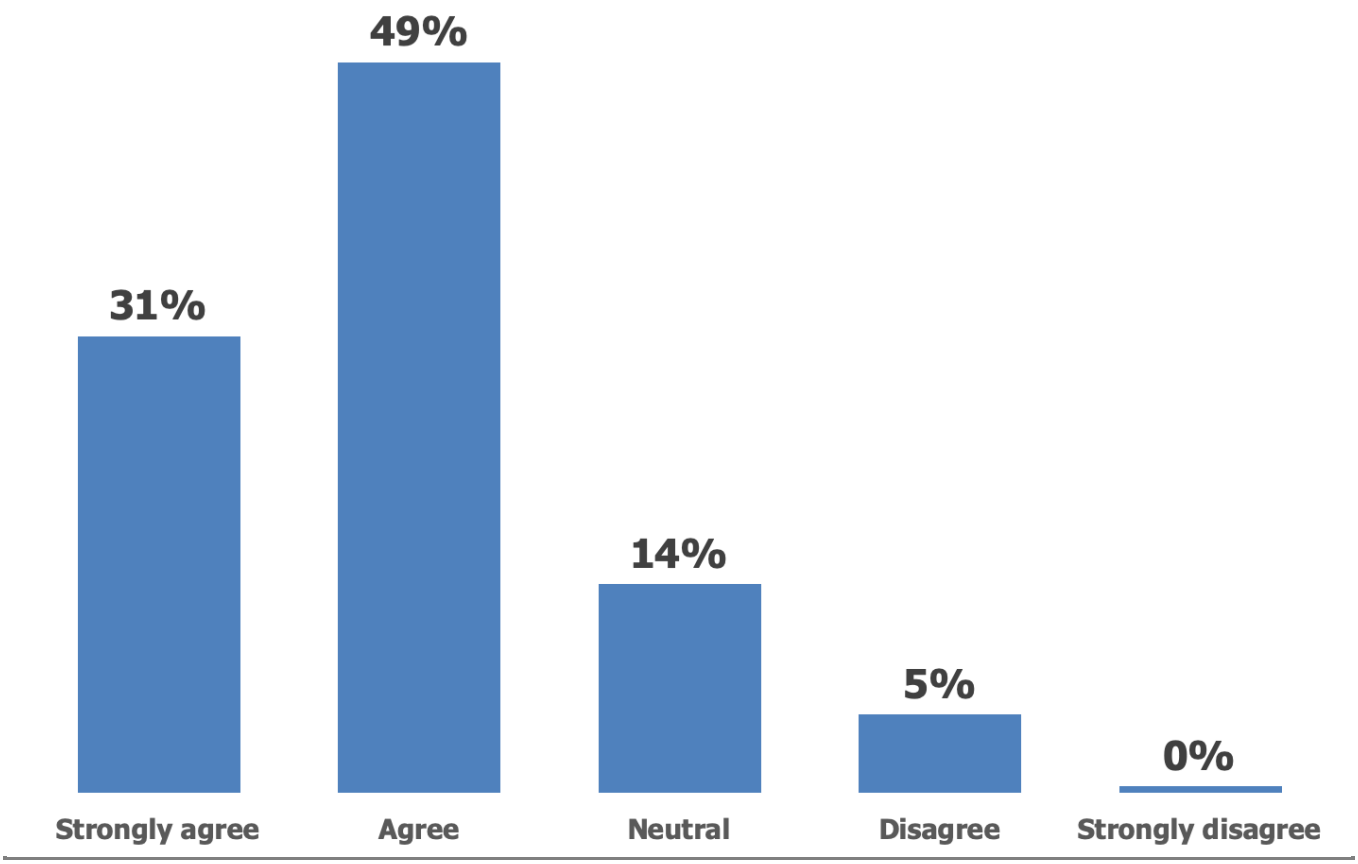
Source: Osterman Research, Inc.

Figure 11
"Does understanding the source of threats allow you to focus on the threats that matter to you?"



Source: Osterman Research, Inc.

Figure 12
Extent to Which Decision Makers Agree Threat Attribution Allows Them to Prepare For and Respond to Threats



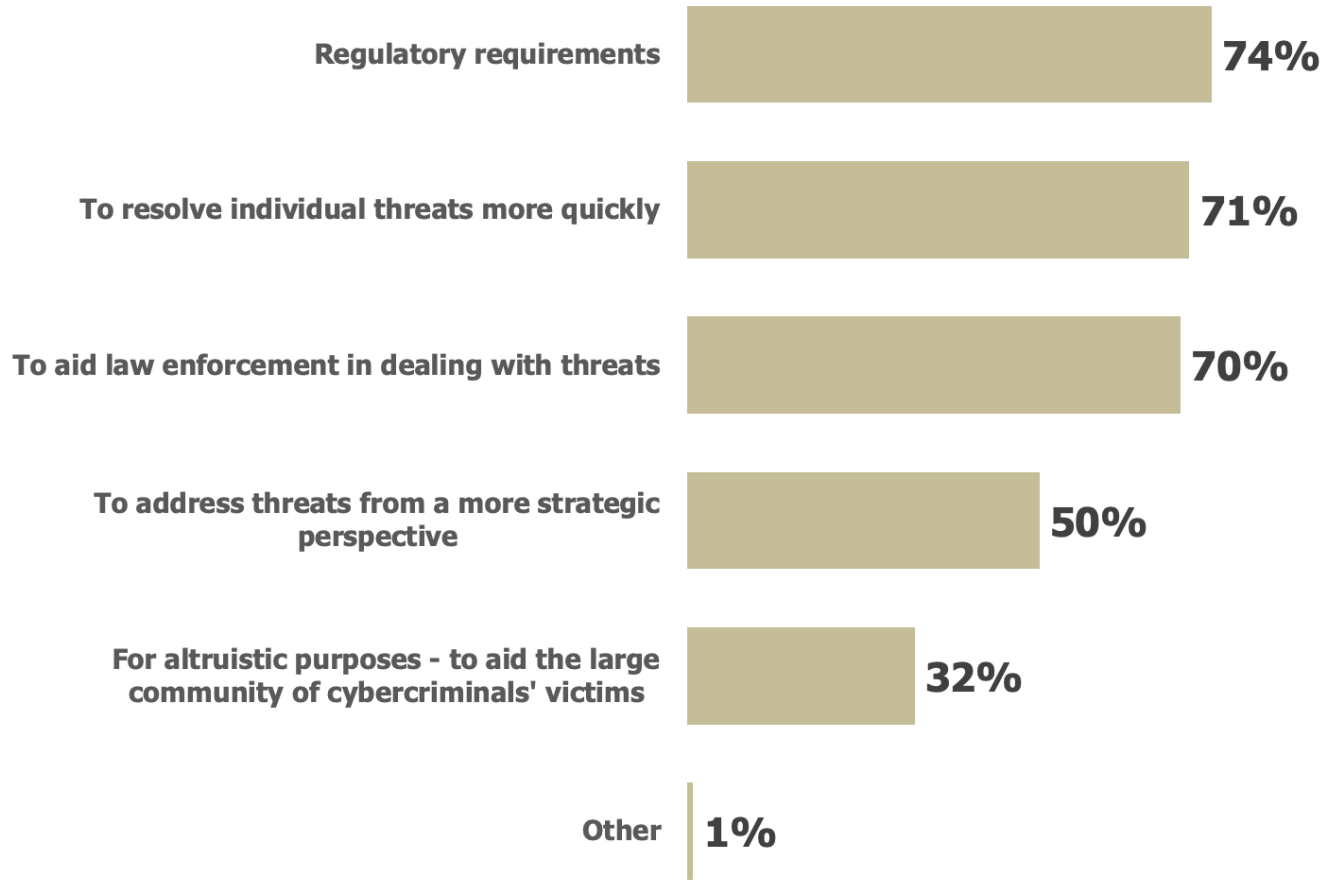
Source: Osterman Research, Inc.

Figure 13
Extent to Which Employees in the Organization are Interested in Threat Attribution
Percentage Responding "interested" or "very interested"

Role	%
IT security management (CISO, head of security, head of security operations, other)	86%
IT management (i.e., CIO, head of IT, head IT architect, other)	79%
IT security non-management (IT security analyst, other options)	75%
Privacy management (i.e., chief privacy officer, other)	65%
IT non-management (operational IT, other)	57%
Finance management (i.e., CFO, finance director, other)	54%
Other non-IT management (director level/other c-suite/business decision maker)	48%

Source: Osterman Research, Inc.

Figure 14
Reasons That Organizations Would Share Information About Threat Attribution Outside of the Organization



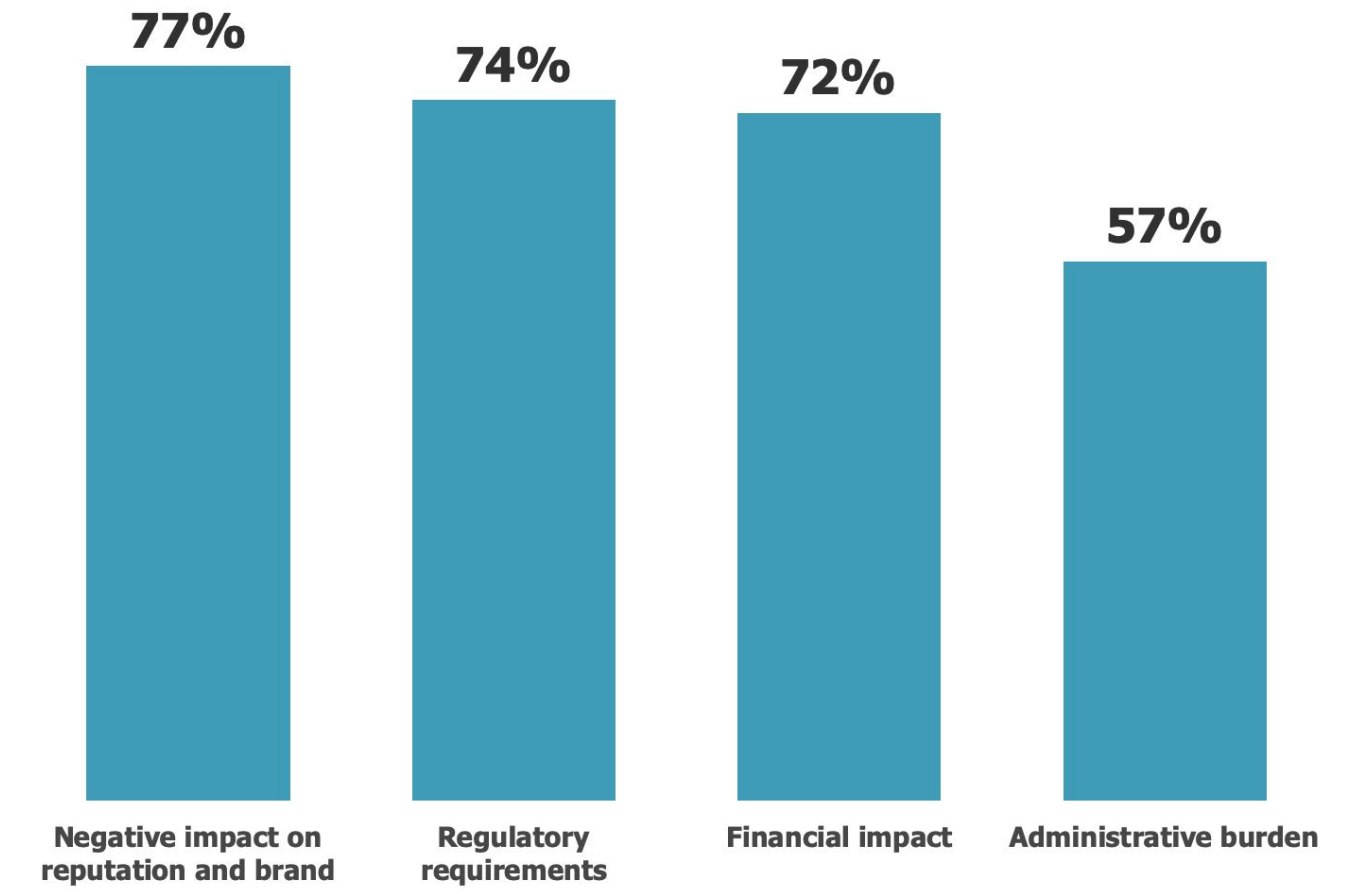
Source: Osterman Research, Inc.

Figure 15
Entities With Which Organizations Share Information About Targeted and Non-Targeted Attacks

	ALWAYS		SOMETIMES		NEVER	
Groups	Targeted	Non-Targeted	Targeted	Non-Targeted	Targeted	Non-Targeted
Law enforcement	43%	28%	53%	62%	4%	10%
Business partners	36%	26%	45%	51%	19%	23%
Security organizations	27%	28%	55%	48%	18%	24%
Peers on an individual basis	11%	5%	48%	62%	41%	33%
Customers	10%	9%	47%	48%	43%	43%
Peer organizations	6%	6%	54%	60%	40%	34%
Independent industry forums	4%	10%	50%	50%	46%	41%

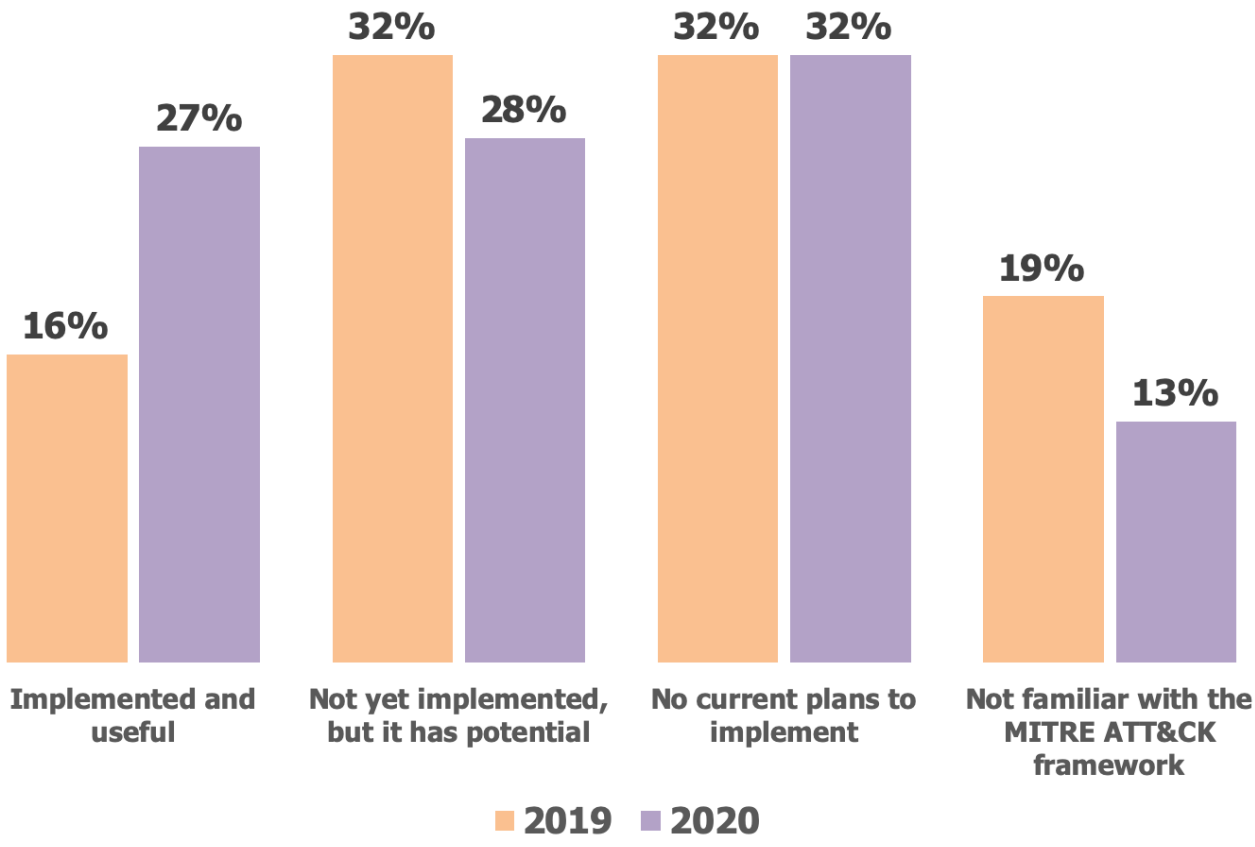
Source: Osterman Research, Inc.

Figure 16
Reasons That Organizations Would Choose Not to Report an Incident to Stakeholders



Source: Osterman Research, Inc.

Figure 17
Perceived Utility of the MITRE ATT&CK Framework for Operationalizing Threat Intelligence, 2019 and 2020



Source: Osterman Research, Inc.

REFERENCES

[i] Source: *New Methods for Solving Phishing, Business Email Compromise, Account Takeovers and Other Security Threats*, Osterman Research, Inc.

[ii] https://www.recordedfuture.com/strategic-threat-intelligence/