

1342345412  
WHITE PAPER

UK



# Building a Threat Intelligence Programme

Research findings on  
best practices and impact

# Methodology



# 351

**total responses**  
from cybersecurity  
decision makers in  
the United States



## FIELD DATES:

March 30th -  
April 4th 2018

APPROXIMATELY



# 15 MINUTE ONLINE SURVEY

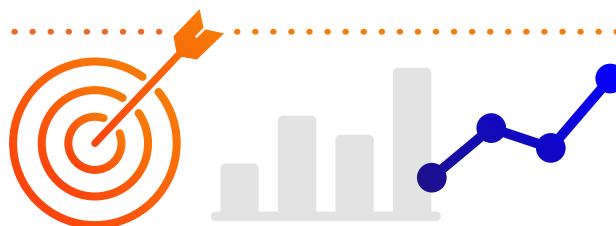
instrument (53 total questions)

Survey respondents  
were provided by  
Branded Research.  
Branded has a  
global reach of  
over **3 BILLION**  
**RESPONDENTS.**



## Overall margin of error +/- 5 POINTS

at a **95%** confidence  
interval



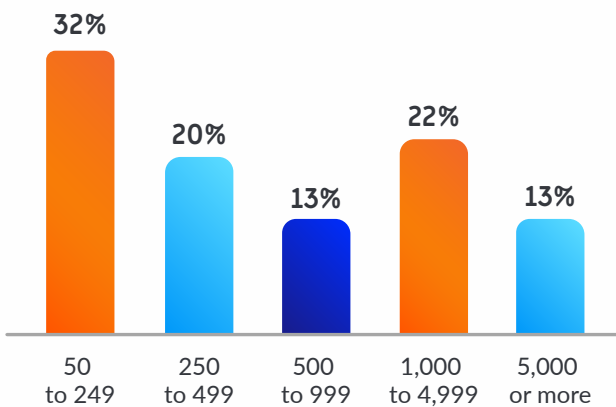
# Demographics

# 100%

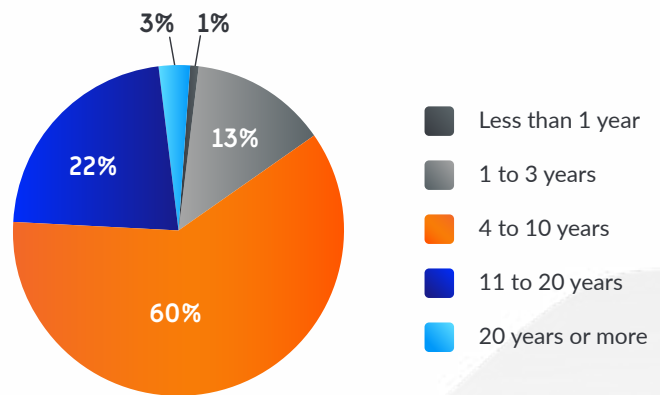
of respondents...

Work **full-time** in IT departments;  
and are **decision makers**  
for **cybersecurity** services,  
technologies, or solution purchases  
within their organizations

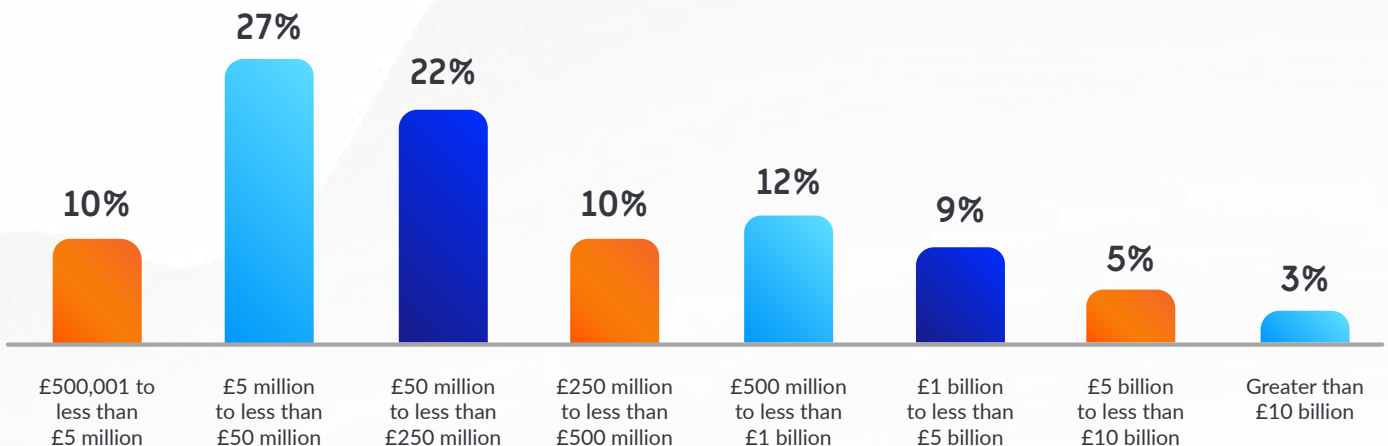
Approximately how many  
employees are in your company at  
all locations worldwide?



How long have you been employed  
in your current role?



In your best estimate, what was your organization's total revenue for last year?



## Current Trends

**“While there are many benefits to implementing a threat intelligence programme, most organisational leaders cite data security (46%) as the primary motivator.”**



“However, less than **one-in-three (28%)** senior managers say the same. Instead, senior managers raise a number of issues, including **risk reduction (24%)** and **compliance (20%).**”

Most commonly, cybersecurity decision makers in organisations with a threat intelligence programme say their organisation developed a threat intelligence programme to deal with data security (42%). Fewer note reducing risk (24%), response to a security incident (15%), compliance (12%), and cost reduction (7%) as motivation for developing a threat intelligence programme.

When describing their organisations' capabilities, almost half (45%) of cybersecurity decision makers surveyed say they are expanding their capabilities and proactively identifying actionable threat intelligence which addresses the 'who', 'why', and 'how' of any given attack to draw further context and connections to refine knowledge. Such organisations may have taken steps to begin automating repetitive tasks, such as data enrichment or indicator aggregation. Data has begun to turn to knowledge.

Nearly two-in-five (35%) cybersecurity decision makers in organisations with a threat intelligence programme report aggregating their threat intelligence information to a platform which enables teams to monitor data in a centralized place. However, the majority (57%) say their organisation uses multiple threat intelligence systems and monitor the data using each tool.

Cybersecurity decision makers (54%) employed by organisations with fully mature threat intelligence programmes report utilizing data aggregation tactics – all data is sent to a threat intelligence platform to be monitored from the centralized tool.



**Nearly two-in-five (35%)**

cybersecurity decision makers in organisations with a threat intelligence programme report aggregating their threat intelligence information to a platform which enables teams to monitor data in a centralized place.



# Building the Programme

**“Nearly one-in-three (31%) cybersecurity decision makers with a threat intelligence programme report it will be another five years or more to build their organisation’s programme to an optimal level.”**



**“In the United Kingdom, half (50%) of organisations with a threat intelligence programme in place say they began building the programme within the last four years.”**

Still, organisations in the United Kingdom are monitoring and interacting with their threat intelligence data constantly. In fact, almost half (46%) of cybersecurity decision makers in organisations with a threat intelligence programme surveyed say their organisation monitors or interacts with its threat intelligence data 24-hours a day. Roughly one-in-five (23%) say their organisation monitors or interacts with its threat intelligence data only a few times a day.

As threat intelligence programmes develop, more time is spent monitoring or interacting with data. Nearly three-in-four (74%) cybersecurity decision makers within organisations with fully mature threat intelligence programmes report interacting or monitoring data 24-hours a day.

In the United Kingdom, cybersecurity decision makers agree – their threat intelligence programmes are working. In fact, more than two-in-five cybersecurity decision makers say their organisation’s threat intelligence programme has prevented phishing attacks (65%), ransomware attacks (56%), breaches of customer data (52%), and business email compromise (46%). Somewhat fewer also note their organisation’s threat intelligence programme has prevented supply chain attacks (39%), insider threats (36%) and nation-state attacks (29%).



**Nearly three-in-four (74%)**

cybersecurity decision makers within organisations with fully mature threat intelligence programmes report interacting or monitoring data 24-hours a day.



In many cases, organisational leaders and those executing day-to-day operations have differing viewpoints when it comes to the rate of success in preventing cyber attacks. In general, organisational leaders are more likely than senior management to say their organisations' threat intelligence programme successfully prevents attacks most of the time, including: phishing attacks (80% vs. 52%), ransomware (74% vs. 49%), breaches of customer data (65% vs. 37%), supply chain attacks (57% vs. 49%), business email compromise (54% vs. 43%) and insider threats (52% vs. 46%).

In fact more than

**two-in-five  
cybersecurity  
decision makers**

say their organisation's threat intelligence programme has prevented phishing attacks (65%), ransomware attacks (56%), breaches of customer data (52%), and business email compromise (46%).



# Managing the Programme

**“In the United Kingdom, cybersecurity decision makers report their organisations are investing heavily in threat intelligence capabilities and teams.”**

Organisations in strong financial health – exceeding more than 10% growth in the last year – are investing even further in threat intelligence capabilities compared to organisations with moderate growth.



## More than two-in-five (43%)

cybersecurity decision makers within fiscally strong organisations, report their organisation invested more than £25 million pounds into their organisations threat infrastructure in the last year, compared to those within organisations (14%) with moderate growth who say the same.

However, further development of threat intelligence is needed – and organisations are planning for it. The majority (51%) of cybersecurity decision makers surveyed indicate their organisations plan to invest more in their threat intelligence infrastructure over the next twelve months. Those within organisations with fully mature threat intelligence programmes must see the value in their programmes because they are even more likely to say they plan to invest more (63%) .

When it comes to further investment, cybersecurity decision makers in telecom and communication services (62%), banking and finance (60%), and retail/ consumer product goods (59%) are more likely than cybersecurity decision makers in manufacturing (44%) or the public sector (36%) to report their organisations’ plans to invest more into threat intelligence infrastructure over the next twelve months.

In the United Kingdom, cybersecurity decision makers indicate a sweeping consensus: threat intelligence training is a necessary component of a successful threat intelligence programme. Nearly two-in-three (63%) cybersecurity decision makers employed by organisations with fully mature threat intelligence programmes say every IT professional within their organisation is trained on the most up-to-date threat intelligence practices.



## 51%


of cybersecurity decision makers surveyed indicate their organisations plan to invest more in their threat intelligence infrastructure over the next twelve months.





Still, nearly two-in-five (37%) say only the IT professionals within their organisation that work specifically with threat intelligence receive any trainings on it.

As expected, cybersecurity decision makers in hi-tech (48%) are more likely to report threat intelligence trainings occurring within their organisation once every few months, compared to those in manufacturing (41%), telecom (38%), and retail/consumer product goods (38%) who say the same.



In the United Kingdom, cybersecurity decision makers indicate a sweeping consensus: threat intelligence training is a necessary component of a successful threat intelligence programme.

**Nearly two-in three  
(63%) cybersecurity  
decision makers**

employed by organisations with fully mature threat intelligence programmes say every IT professional within their organisation is trained on the most up-to-date threat intelligence practices.





# Interplay – Private & Public Organisations

**“In the United Kingdom, more than three-in-five (61%) cybersecurity decision makers report that their organisations look to governments to help provide information or data about cyber threats (compared to 68% in the US).”**



## **“Roughly the same (60%)**

**say the government has programmes designed to assist companies in combating cybersecurity threats (compared to 68% in the US).”**

Those who believe their organisations' threat intelligence programmes are behind industry standards may be more reliant on help from government bodies. Seven-in-ten (70%) cybersecurity decision makers who look to governments to help provide data or information about cyber threats describe their organisation's threat intelligence programme to be behind industry standards.

As such, organisations in the United Kingdom are accustomed to working in tandem with government groups to combat cyber threats. More than one-in-three (38%) cybersecurity decision makers report their organisation shares its threat intelligence data with a government group (compared to 36% in the US). Fewer (21%) say their organisation shares its threat intelligence data with an NGO.

Still, one-in-three (33%) cybersecurity decision makers indicate their organisation does not share information externally (compared to 39% in the US).

More than two-in-five cybersecurity decision makers report sharing malware data (49% vs. 54% US), general threat data (44% vs 47% US), ransomware data (42% vs. 43% US), DDoS or DoS data (41% vs. 45% US), and real-time threat data (40% vs. 40% US) with government groups or NGO's.

In the United Kingdom, nearly four-in-five (79%) cybersecurity decision makers agree a better relationship with government groups would foster a better environment for exchanging threat intelligence data (compared to 84% in the US).



## **One-in-three (33%)**

cybersecurity decision makers indicate their organisation does not share information externally (compared to 39% in the US).



## ADDITIONAL DATA

## Interplay – Private & Public Organisations

- Two-in-three (66%) cybersecurity decision makers agree governments do an excellent job of providing real-time threat data to help their organisations when they are being attacked.
- Sharing data with government groups is a priority for many organisations. With all of the cyber threats that surface each day, seven-in-ten (70%) cybersecurity decision makers agree that coordinating data sharing with governments is one of the main priorities in further development of their organisations' threat intelligence protocol.



### Seven-in-ten (70%)

cybersecurity decision makers agree their organisation is **more secure** because of the information they receive from governments about cybersecurity threats.

- Still, seven-in-ten (70%) cybersecurity decision makers employed by organisations with fully mature threat intelligence programmes agree – with all of the additional cyber threats faced each day, coordinating data sharing with governments is one of their main priorities – indicating collaborative practices between private enterprise and governments groups is still a concept in infancy.
- More than one-in-three cybersecurity decision makers say there are many things governments can do to help ensure sharing threat intelligence information between private and public entities is valuable, including: creating and distributing defensive tools and techniques to companies to help combat known cyber-attacks (45%), providing regular briefings for cybersecurity employees about the most recent trends in cyber-attacks (44%), providing clear guidance for how and when to share data (43%), creating industry groups that are tasked with working on cybersecurity threats that are specific to each industry (43%), assisting companies in actively combating nation-state attackers (39%), offering more granular information about specific threats that companies face (38%) and setting up bounty programmes to pay organisations for cyber-attack attribution data (36%).



Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit [www.ThreatConnect.com](http://www.ThreatConnect.com).

[ThreatConnect.com](http://ThreatConnect.com)

3865 Wilson Blvd., Suite 550  
Arlington, VA 22203

[sales@threatconnect.com](mailto:sales@threatconnect.com)

1.800.965.2708