SOPHOS

The Role of Law Enforcement in Remediating Ransomware Attacks

Insights from 2,974 organizations that were hit by ransomware in the last year

A Sophos Whitepaper. May 2024

Introduction

In the early years of ransomware, many (if not, most) victims were reluctant to admit publicly that they had been hit for fear of exacerbating the business impact of the attack. Concerns about negative press and customer attrition led many organizations to keep quiet.

More recently, the situation has changed, with ransomware victims increasingly willing to acknowledge an attack. This development is likely driven in part by the normalization of ransomware – our (wholly anonymous) State of Ransomware reports have revealed attack rates above 50% for the last three years and public acknowledgement of an attack by well-known brands is commonplace. In short, being hit by ransomware is no longer perceived to be an automatic badge of shame.

The increase in mandatory reporting of attacks in many jurisdictions is also likely driving greater disclosure, particularly in the public sector which is most impacted by these regulations and requirements.

Although there has been a general sense that reporting has increased, detailed insights and regional comparisons have been hard to come by – until now. This year's Sophos State of Ransomware survey shines light into this area, revealing for the first time how reporting levels and official responses vary across the 14 countries studied.

Reporting a ransomware attack is a win-win

The nature and availability of official support when dealing with a ransomware attack vary on a country-by-country basis, as do the tools to report a cyberattack. U.S. victims can leverage the Cybersecurity and Infrastructure Security Agency (CISA); those in the UK can get advice from the National Cyber Security Centre (NCSC); and Australian organizations can call on the Australian Cyber Security Center (ACSC), to name but a few.

Reporting an attack has benefits for both the victim and the official bodies that look to support them:

- **Immediate remediation support**: Governments and other official bodies are often able to provide expertise and guidance to help victims remediate the attack and minimize its impact
- **Policy guidance insights**: Protecting businesses from cybercrime, including ransomware, is a major focus for many governments around the globe. The more insights officials have into attacks and their impact, the better they can guide policies and initiatives
- **Attacker takedown enablement**: Timely sharing of attack details assists national and pan-national efforts to takedown criminal gangs, such the Lockbit operation in February 2024

With these benefits in mind, the insights from the survey make encouraging reading.

Insight 1: Most ransomware attacks are reported

Globally, 97% of ransomware victims in the last year reported the attack to law enforcement and/or official bodies. Reporting rates are high across all countries surveyed with just ten percentage points between the lowest rate (90% - Australia) and the highest (100% - Switzerland).

The findings reveal that, while annual revenue and employee count have minimal impact on propensity to report an attack, there are some variations by industry. In sectors with high percentages of public sector organizations, almost all attacks are reported:

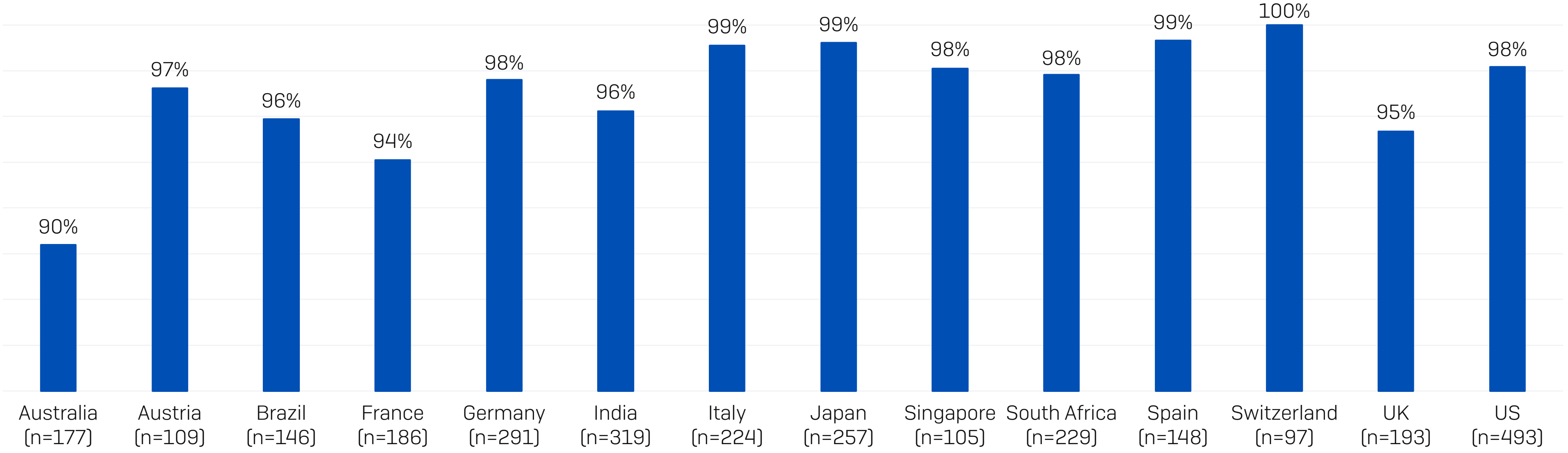
- 100% state and local government (n=93)
- 99.6% healthcare (n=271)
- 99.5% education (n=387)
- 99.4% central/federal government (n=175)

Distribution and transport has the lowest reporting rate (85%, n=149), followed by IT, technology and telecoms (92%, n=143).

Insight 2: Law enforcement almost always provides support

For the organizations that do report the attack, the good news is that law enforcement and/or official bodies almost always get involved. Overall, just 1% of the 2,974 victims surveyed said that they did not receive support despite reporting the attack.

Propotion of ransomware attacks reported to law enforcement and/or official bodies



If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? (n=2,974 organizations hit by ransomware in the last year)

Insight 3: Support provided to ransomware victims varies by country

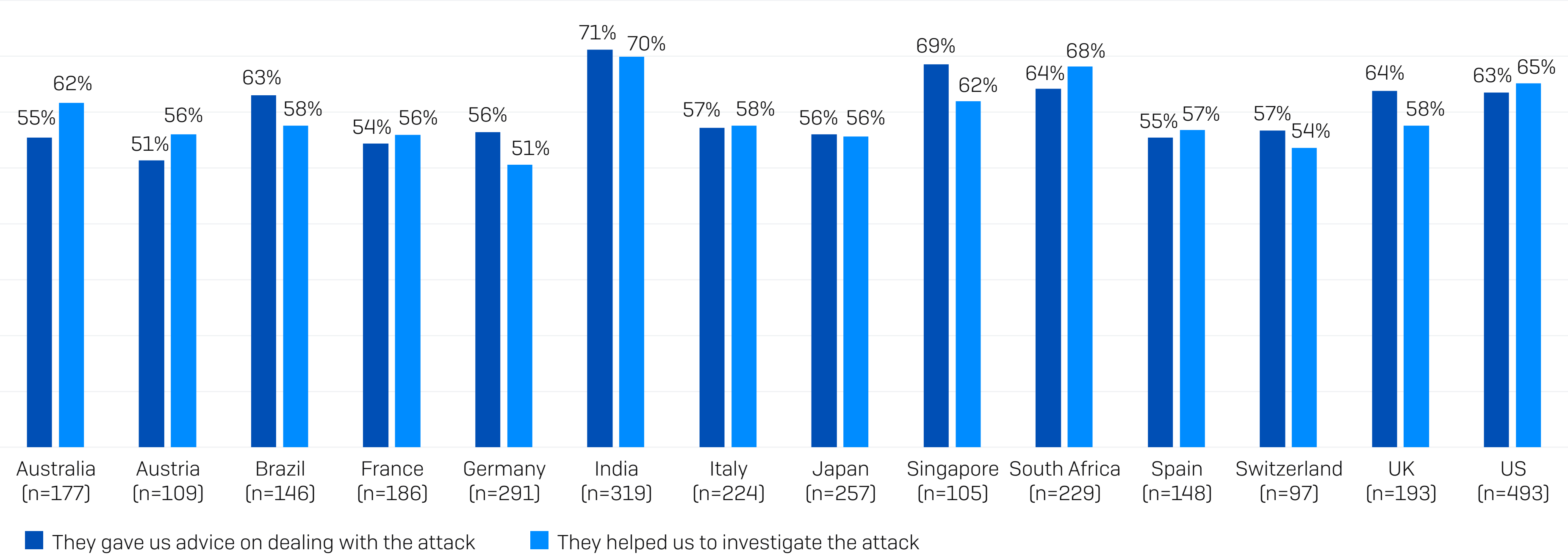
Respondents that reported the attack received support in three main ways:

- Advice on dealing with the attack (61%)
- Help investigating the attack (60%)
- Help recovering data encrypted in the attack (40% of all victims and 58% of those that had data encrypted)

Diving deeper, we see that the exact nature of law enforcement and/or official body involvement varies according to where the organization is based. While more than half of victims *received advice on dealing with the attack* across all countries surveyed, organizations in India (71%) and Singapore (69%) reported the highest level of support in this area.

Indian respondents also reported the highest level of *support in investigating the attack* (70%) followed by those in South Africa (68%), while the lowest rate was reported in Germany (51%).

Provision of official advice and/or help investigating the ransomware attack



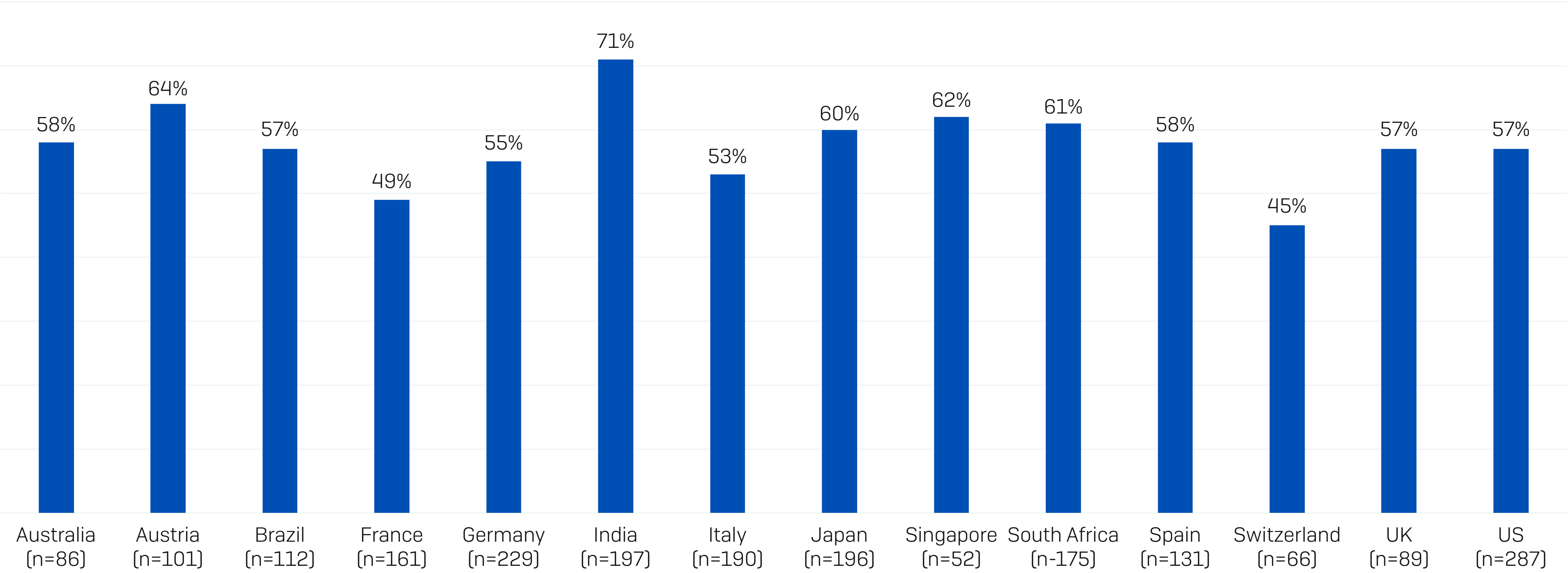
If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? (n=2,974 organizations hit by ransomware in the last year)

Assistance recovering encrypted data

Among those that had data encrypted, more than half globally (58%) received support in recovering their encrypted data.

India continues to top the chart, with 71% of those that had data encrypted receiving assistance in recovering it. Notably the countries with the lowest propensity for victims to receive help recovering encrypted data are all in Europe: Switzerland (45%), France (49%), Italy (53%) and Germany (55%).

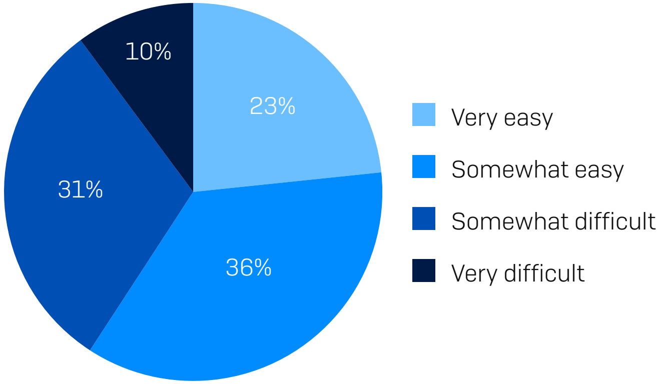
Assistance recovering encrypted data



If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? (n=2,072 organizations hit by ransomware in the last year and that had data encrypted)

Insight 4: Engaging with law enforcement is generally easy

Encouragingly, more than half (59%) of those that engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (23% very easy, 36% somewhat easy). Only 10% said the process was very difficult, while 31% described it as somewhat difficult.

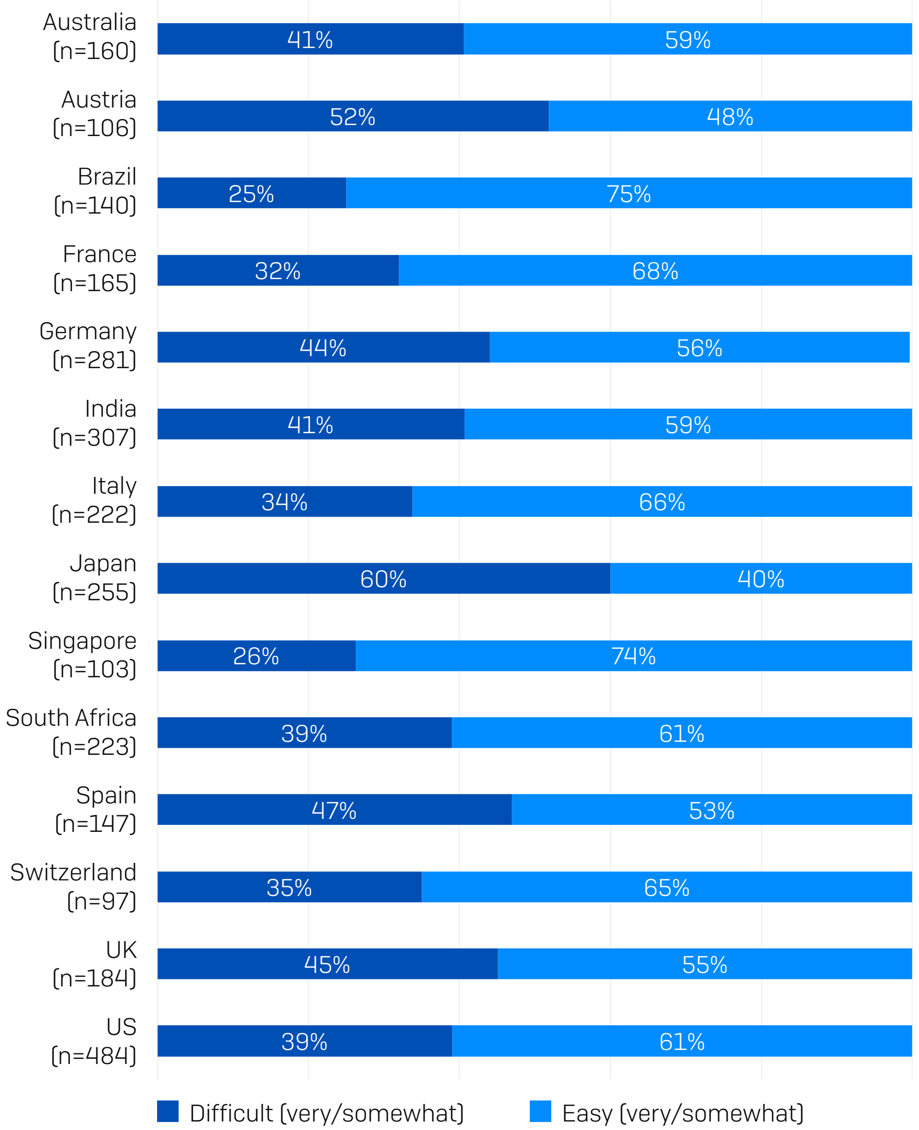


How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=2,874 (excluding 'don't know' responses).

Ease of engagement also varies by country. Those in Japan were most likely to find reporting difficult (60%), followed by those in Austria (52%). Japanese respondents also had the highest propensity to find it "very difficult" to report the attack (23%)

Conversely, respondents in Brazil (75%) and Singapore (74%) were most likely to find it easy to engage, while Italian organizations had the highest percentage that found it "very easy" (32%).

Ease of engagement with law enforcement



Insight 5: There are myriad reasons attacks are not reported

There were a range of reasons why 3% (86 respondents) did not report the attack, with the two most common being concern that it would have a negative impact on their organization, such as fines, charges, or extra work (27%), and because they did not think there would be any benefit to them (also 27%). Several respondents provided verbatim feedback that they did not engage official bodies as they were able to resolve the issue in-house.

REASON FOR NOT REPORTING ATTACK	PERCENTAGE
We were concerned that it would have a negative impact on our organization e.g., fines, charges, extra work	27%
We did not think there would be any benefit to our organization to report the attack	27%
We did not think they would be interested in the attack	22%
We were too busy dealing with the attack to think about involving them	21%
The attackers warned us not to engage them	19%
We did not know which law enforcement or official bodies to involve	10%
We were not legally required to report the attack	9%
Other (please specify)	3%
Don’t know	1%

Why didn’t you report the attack to law enforcement and/or official bodies? (n=86 organizations hit by ransomware in the last year that didn’t report the attack.)

Conclusion

The survey findings have revealed that reporting of ransomware attacks is very common, and victims almost always receive support as a result. Hopefully, these findings will encourage any organization that does fall victim in the future to notify their relevant body/ies. While it is generally easy for organizations to report an attack, there are also opportunities to facilitate the process at what is, inevitably, a very stressful time. As Chester Wisniewski, director, Global Field CTO, Sophos, comments:

> *"Criminals are successful in part due to the scale and efficiency with which they operate. To beat them back, we need to match them in both these areas. That means that, going forward, we need even greater collaboration, both within the private and public sector—and we need it at a global level."*

About the survey

The Sophos State of Ransomware 2024 report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. All respondents represent organizations with between 100 and 5,000 employees.

The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants were asked to respond based on their experiences over the previous year. Within the education sector, respondents were split into lower education (catering to students up to 18 years) and higher education (for students over 18 years).

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

© Copyright 2024. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2024-05-10 WP-EN (PC)

SOPHOS