ACAMS

Global Ransomware Risks Survey

Report Published: March 2022

Contents

Disclaimer and Acknowledgements

ACAMS thanks its global community spread across 180 countries/ regions, and its global chapters network for being part of this landmark initiative.

This report would not have been possible without the sponsorship, guidance and support of Dr. Justine Walker, Global Head of Sanctions, Compliance and Risk, with thanks also to Lauren Kohr, Senior Director AML, Americas, for her significant partnership and support throughout the project.

A special acknowledgement also goes to Lashvinder Kaur, Vice President of Global Strategic Communications, the ACAMS Marketing, Global Operations, Chapters, and Communications teams for supporting this project.

Introduction

ACAMS is pleased to present this unique Global Ransomware Risks survey, carried out in partnership with YouGov. We are extremely grateful to those in the private and public sectors who offered their personal perspectives on this area.

As with any survey, it should be recognized that there are certain limitations. Individuals may choose to opt in or opt out of participation and those who participated may not fully replicate the global picture. The survey was conducted by a respected independent research agency who followed the Market Research Society's code of conduct. As such, the findings can be taken to offer an illustrative view and the results do provide a rare insight into both the challenges and opportunities that the public and private sector face in addressing the complexities of ransomware.

Ransomware is a relatively new area to the anti-financial crime (AFC) community. While attacks have been going on for many years, the COVID-19 pandemic and the resulting move to a more digital world have greatly increased organizational and individual exposure and vulnerability to ransomware. Alongside this, national governments have increasingly focused attention on combatting the ransomware ecosystem, including through the use of anti-financial crime measures such as sanctions. Demonstrating this increased focus, a recent Joint Statement by over 30 countries declared ransomware to be an "escalating global security threat with serious economic and security consequences". Amid this evolving threat landscape, it is critical for organizations to adequately understand their risk and take proactive and appropriate steps to mitigate these risks.

Furthermore, as the financial sanctions tool is increasingly used against criminal cyber actors by various jurisdictions, there is a heightened probability of a sanctions nexus should a ransomware payment be made. Our purpose in conducting this survey is primarily to gain an insight into industry and government perceptions of, and resilience to, ransomware financial crime risks, as well as identifying the areas where further training or dialogue would be most useful.

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives. Visit acams.org for more information.

Author

Sam Cousins is a Sanctions and Risk Associate at ACAMS.

Executive Summary and Key Findings

This survey has found that the prevailing view among respondents is that ransomware does pose a threat to their organization and that the threat is growing, but it is not seen as the biggest current cyber threat. Additionally, respondents are split on considering ransomware sanctions risks within their sanctions compliance program, with only a small number of respondents stating that they are familiar with the potential sanctions risks associated with making ransomware payments. The vast majority of respondents believe their national government needs to do more to protect businesses against ransomware, and that the most useful action to advance the global fight against ransomware is to identify and penalize ransomware groups.

Summary of Key Findings

Familiarity with ransomware

48% of respondents consider themselves to be familiar with ransomware, and the same number are familiar with the legal obligations for ransomware payments under local law.

Attitude towards ransomware

38% of respondents believe that ransomware payments should never be made under any circumstance. 85% agree that payment of ransomware encourages further attacks.

Notification of law enforcement

80% would proactively notify law enforcement in the event of an attack.

Threat of ransomware

12% of respondents view the current ransomware threat to their organization as very high, 20% view it as high, 26% as moderate, 17% as low, and 11% as very low.

65% view the threat of ransomware as increasing, compared to 2% who view it as diminishing. Despite this, only 8% view ransomware as the greatest cyber threat their organization faces. 47% believe a ransomware attack is likely in the next 12 months.

9% of those surveyed had suffered a successful ransomware attack.

Sectors at risk

The financial sector was seen as most at risk of ransomware attacks, with 77% of respondents viewing it as high risk. This was followed by government at 65%, and technology at 57%.

Geographical risk

The jurisdictions deemed most likely to be the origin point of a ransomware attack were Russia (58%), China (55%), and the US (31%).

Integration of ransomware sanctions risks

42% of respondents from financial institutions (FIs) consider ransomware sanctions risks as part of their sanctions compliance program (SCP). For non-FIs with SCPs, 38% consider ransomware sanctions risks within it.

Awareness of ransomware sanctions risks

Just under a quarter of FI respondents consider themselves familiar with the sanctions risks from making ransomware payments to cyber criminals, with 34% stating they are not at all familiar. Non-FI respondents were slightly higher, with 28% considering themselves familiar.

Protection from ransomware

84% of respondents consider their organizations to be at least adequately protected from ransomware attacks, with over half of this number believing more could be done. Only 5% felt their organization is inadequately protected. 61% state their organization has taken additional steps over the past 12 months to protect itself from ransomware.

Cyber incident response plan

58% of respondents have a cyber incident response plan in place for ransomware attacks, with 81% of these respondents believing it to be effective.

The role of anti-financial crime (AFC) professionals in ransomware response

Only 58% of respondents require anti-money laundering (AML) professionals' participation as part of their cyber incident response plan, and only 40% of respondents require sanctions compliance personnel. Only a quarter of respondents state a process has been developed where a potential ransomware attack should be elevated to the AFC department.

Policies, procedures, and training

Under 50% of respondents have policies and procedures on ransomware-related risk management, anti-financial crime training which addresses ransomware, or other training which addresses ransomware risks.

Insurance

53% of respondents who have ransomware insurance are aware of the terms of their ransomware insurance and what measures need to be taken to comply with it.

National government efforts

Only 20% of respondents view their government as doing at least an adequate job at safeguarding private sector organizations against ransomware attacks. 37% state that their government has conducted no outreach on how to report and respond to ransomware attacks.

Respondents believe that stronger efforts by governments to identify and penalize ransomware groups would be the most effective way to advance the global fight against ransomware, with 79% of those surveyed viewing this as useful. The next most useful actions identified are greater flexibility within the public and private sectors to share relevant intelligence (77%) and stronger training throughout the private sector on how to shield organizations from attacks (77%).

Key informational needs

Respondents particularly emphasized the usefulness of greater access to specific information on current and emerging ransomware threats (76% of those surveyed), the issuance of guidance on how to best prevent ransomware attacks (75%), and more flexibility to share data on ransomware attacks with peer institutions (70%).

The most important training topics were identified as compliance and red flag indicators of ransomware (85% of those surveyed classifying it as important), integrating cybersecurity with AFC/sanctions compliance (83%), training on mitigating ransomware-related sanctions risks (82%), and ransomware 101 training (80%).

Prohibition of ransomware

38% of respondents believe ransomware payments should be banned in all cases, with 32% believing that they shouldn't, and 29% unsure.

Methodology

This report is based on 395 unique responses from the global compliance community, received between October 28 and December 6, 2021. Respondents were asked where they are based, the type of organization they work for, and their role.

Geographical Distribution

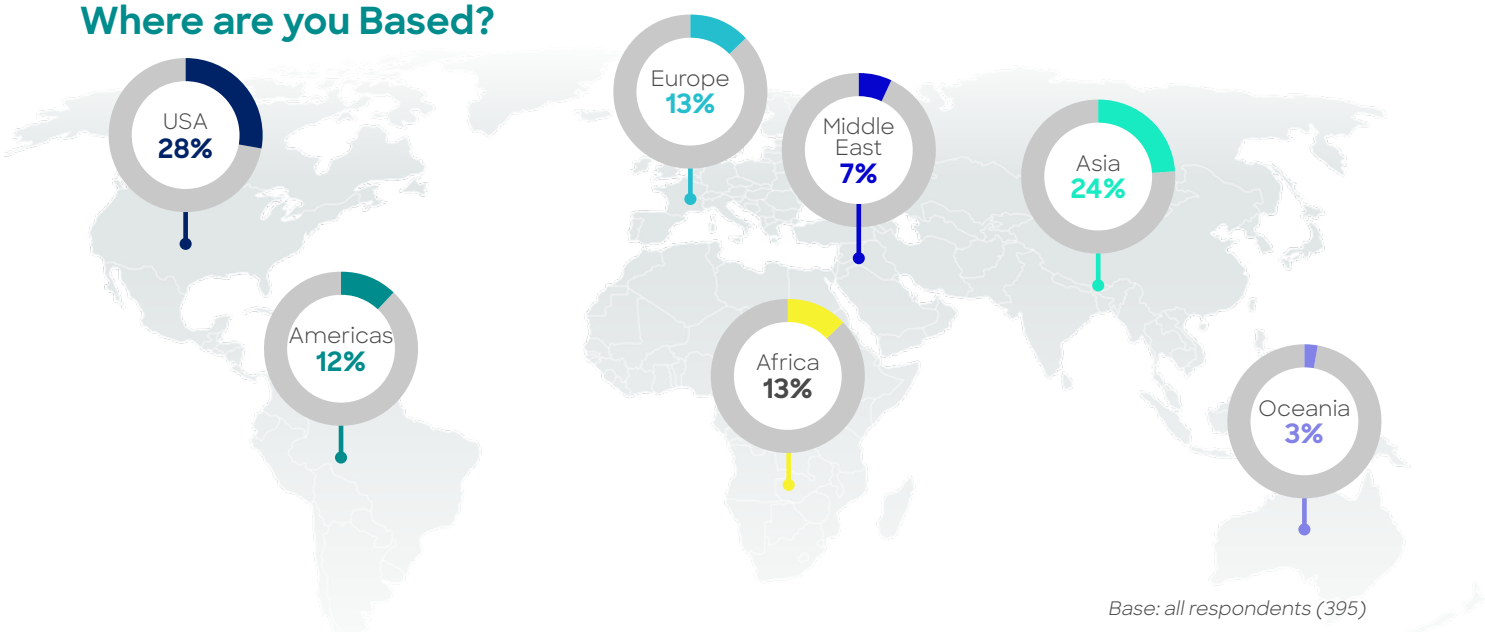
The geographical distribution of survey respondents is as follows:

- 28% of respondents are based in the USA, 24% in Asia, 13% in Africa, 12% in the Americas (excluding the USA), 13% in Europe, 7% in the Middle East, and 3% in Oceania

- Non-government respondents were also asked where their institution is headquartered, with the results showing 30% headquartered in the USA, 20% Asia, 18% Europe, 12% Americas (excluding the USA), 10% Africa, 8% Middle East, and 2% Oceania

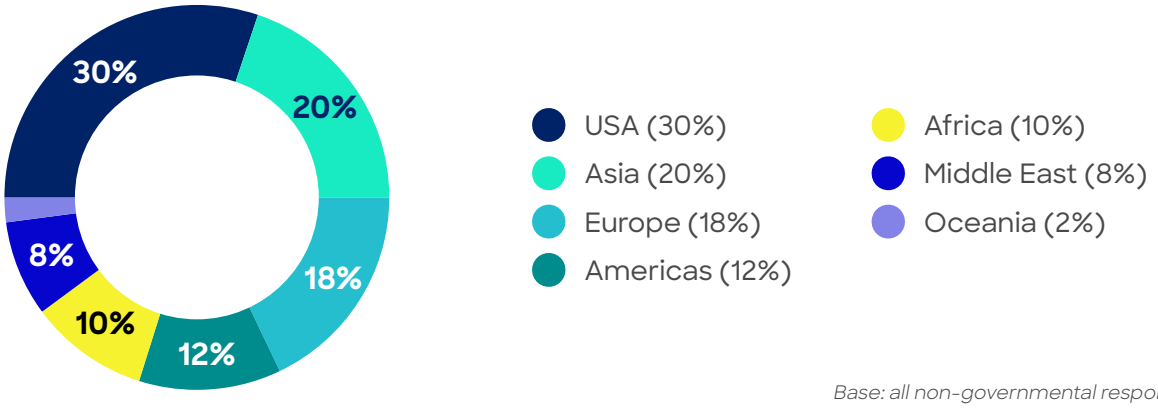
Due to this healthy geographic split, this report will include regional breakdowns for certain questions, though Oceania will not be included as we received insufficient responses for this to be statistically significant.

Where are you Based?



Base: all respondents (395)

Where is Your Institution Headquartered?



Base: all non-governmental respondents (348)

Industry

By way of industry, the majority of respondents work in financial institutions (64%), with an additional 12% working in government. The remaining 24% comprised of corporates, education and healthcare, law firms, cyber firms, those from the crypto industry, and other organizations. In analyzing this data, we will group these respondents together as "non-FI" respondents.

Almost two thirds of respondents work for financial institutions, whilst over one in ten work for government organizations.

64%
Financial institution

24%
Non-FI private sector

12%
Government

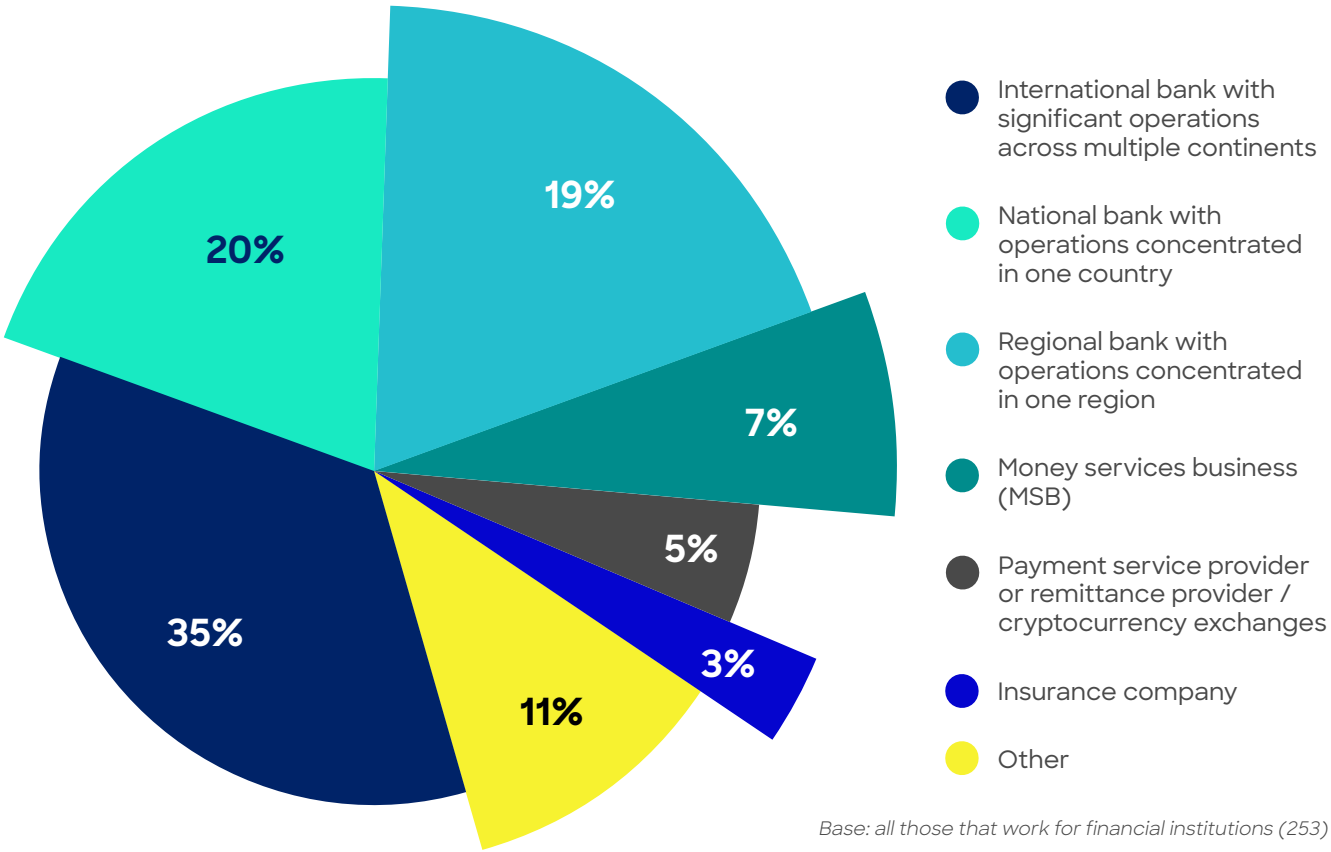
Base: all respondents (395)

Type of Institution

The survey asked FI respondents to identify the type of institution they work in. These financial institution respondents comprised of those working for international banks (35%), regional banks (19%), national banks (20%), MSBs (7%), and others.

Over a third of financial institution respondents categorise their institutions as an international bank.

How would you categorise your institution?



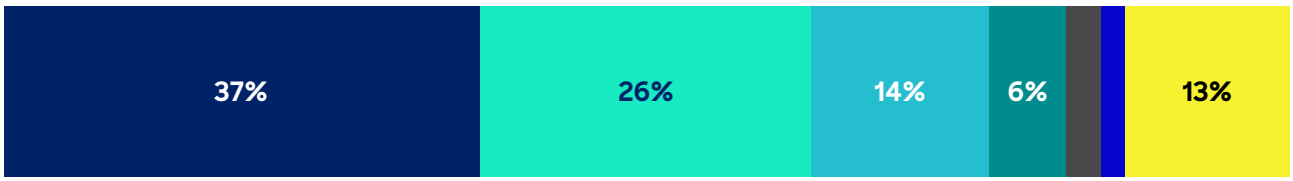
Base: all those that work for financial institutions (253)

Roles

FI respondents were also asked their role – 37% are mid-to-junior level in compliance, 26% senior management in compliance, 14% legal/regulatory/risk management, 6% executive leadership, 13% other.

Over a quarter of financial institution respondents have senior management compliance positions, whilst over a third are mid-to-junior level.

Which of the following best describes your position?



- Mid-to-junior level in compliance
- Senior management in compliance
- Legal/regulatory/risk management
- Executive leadership
- Trade finance
- Cyber security/IT systems
- Other

Base: all those that work in financial institutions (253)

Terminology

In assessing the data, this report will use a number of terms to refer to segments of respondents. To clarify, "industry" will be used to refer to all non-government respondents. "FI respondents" refers to those who selected "financial institution" as their organization, and "non-FI respondents" refers to those who are from the private sector but not at a financial institution. This latter category includes, for example, actors in the cryptocurrency industry, energy, and retail organizations.

Familiarity With and Attitude Towards Ransomware

The survey asked respondents a number of questions regarding their familiarity with ransomware, as well as their attitude towards it.

Of those responding to the survey, just under half (48%) considered themselves to be familiar with ransomware, with the same percentage of respondents stating that they are familiar with the legal obligations regarding ransomware payments.

Respondents were asked questions on their attitude to ransomware, including perceptions regarding payment. Over a third (38%) stated that ransomware payments should never be made under any circumstances. 36% stated payments are acceptable if there is a national security risk, and 29% if there is substantial reputational and operational risk. 6% indicated that ransomware payment should be considered in any circumstances provided it isn't legally prohibited.

85% of respondents agreed that paying a ransom to hackers encourages further attacks, with 59% strongly agreeing with this.

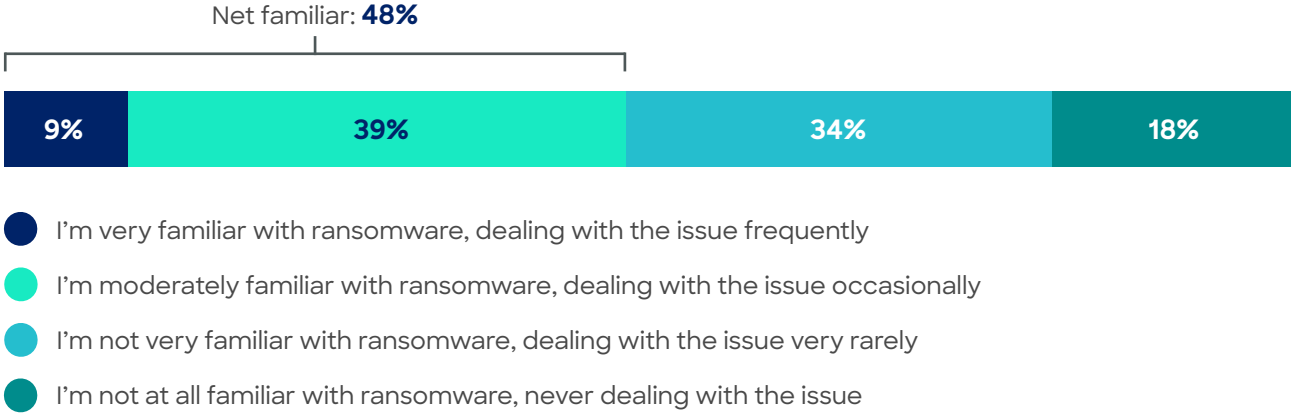
80% of industry respondents stated that they would proactively notify law enforcement in the event of a ransomware attack, with only 1% selecting no, and 14% stating that it would depend on the situation. Further breakdown of scenarios showed that risk to human life (83%) and national security risks (75%) were the most likely scenarios in which law enforcement would be proactively contacted.

ACAMS Observations

While half of respondents are unfamiliar with ransomware, the strong majority would proactively notify law enforcement in the event of an attack. Although the strong majority of respondents feel that payment encourages further attacks, they are split on which scenarios justify payment of ransom, with less than half believing they should never be paid.

Almost half of the respondents say they are familiar with ransomware, while just under one in five say they never deal with the issue.

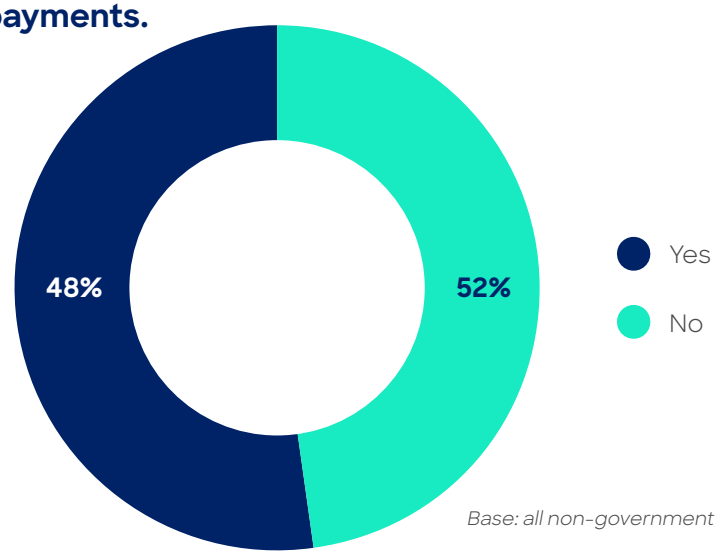
How would you characterize your knowledge of ransomware?



Base: all respondents (395)

Respondents are evenly split when it comes to being familiar with their obligations regarding ransomware payments.

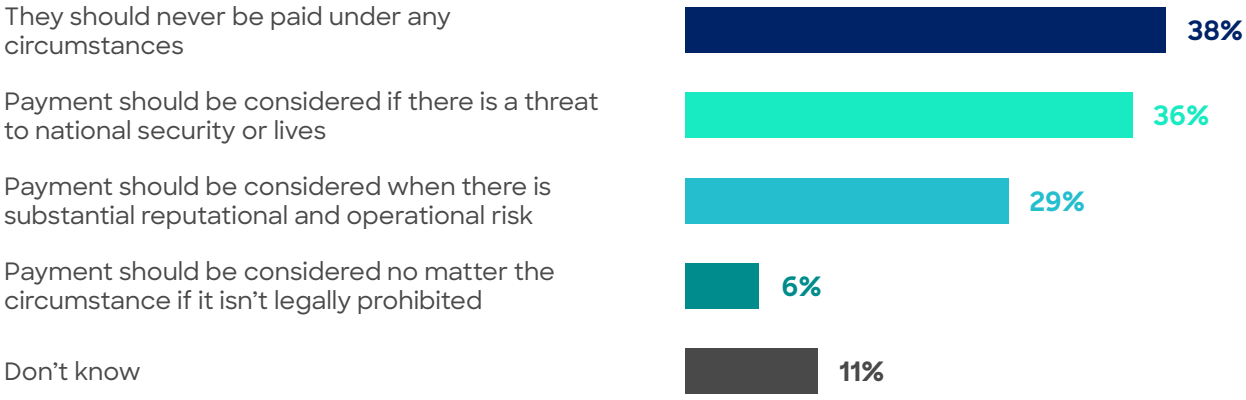
Are you familiar with your obligations under local law regarding ransomware payments?



Base: all non-government respondents (348)

Over a third of respondents believe that payments to hackers should never be made under any circumstances.

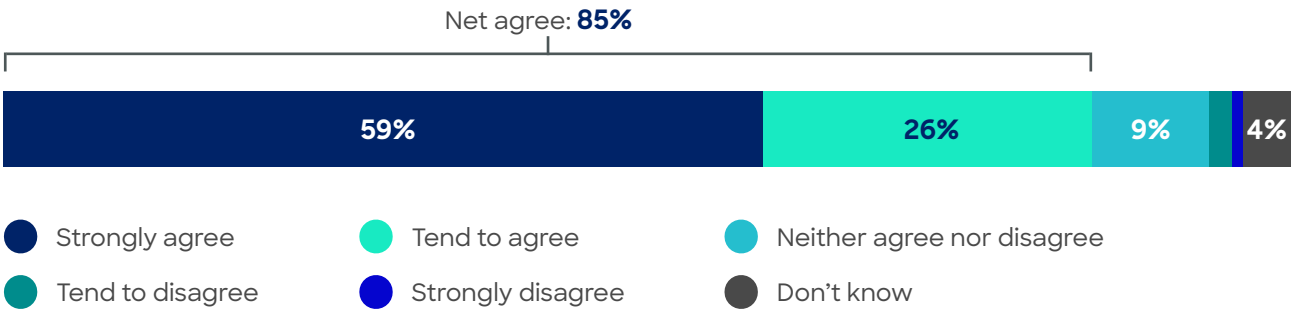
Which of the following best describes your attitude toward ransom payments to hackers?



Base: all respondents (395)

Over eight in ten respondents agree with the statement that paying a ransom to hackers encourages further attacks.

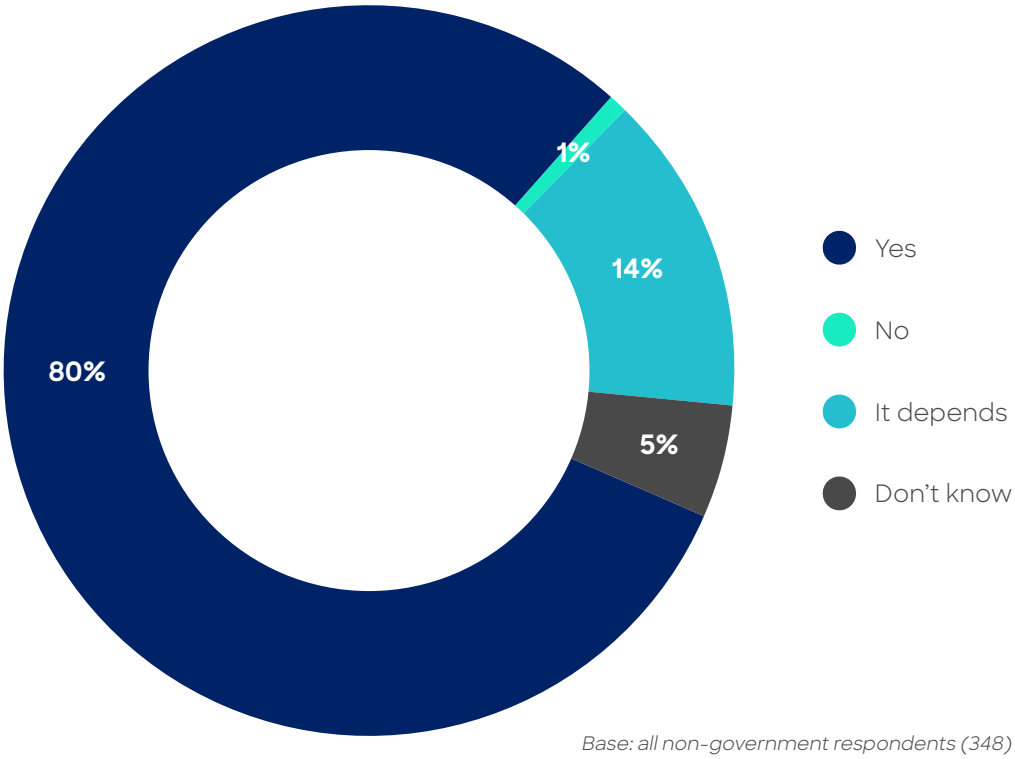
To what extent do you agree or disagree with the statement that paying a ransom to hackers encourages further attacks?



Base: all respondents (395)

Eight in ten industry respondents would proactively notify law enforcement in the event of ransomware attacks.

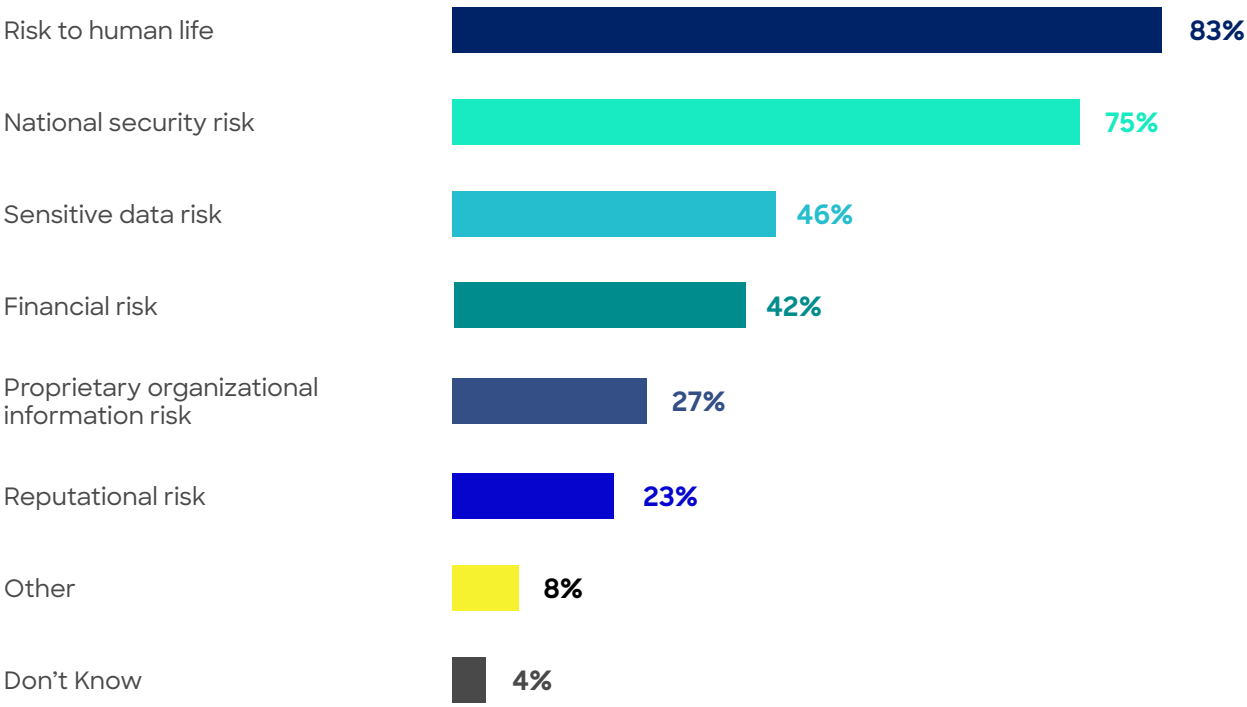
Would you proactively notify law enforcement in the event of ransomware attacks?



Base: all non-government respondents (348)

Of those that are uncertain whether they would proactively notify law enforcement, over three quarters say they would notify law enforcement if there was a risk to human life or a national security risk.

In which of the following cases, if any, would you proactively notify law enforcement?



Base: all non-government respondents who say "it depends" re. whether they would proactively notify law enforcement (48)

Ransomware Threat Landscape

The survey asked respondents a number of questions on how they perceive the threat of ransomware. While ransomware is seen as at least a moderate threat to their organization by over 50% of respondents, only 32% categorized it as either “high” or “very high”.

This perception may change over time however, as 65% of respondents view ransomware as a growing threat, with only 2% stating that the threat is diminishing to their organization. Indeed, 47% of respondents felt that their organization is either likely or highly likely to be the target of a ransomware attack in the next 12 months. Despite this, only 8% of respondents view ransomware as the greatest cyber threat to their organization, with 51% viewing it as one of several high-priority threats. In comparison, only 10% described it as a minor concern compared to other cyber threats.

When asked which sectors are most at risk of ransomware attacks, respondents generally find finance, government, and technology to be most at risk, being viewed as the highest risk by 77%, 65%, and 57% of respondents respectively. Only 12% and 22% viewed education and retail as the highest risk, respectively.

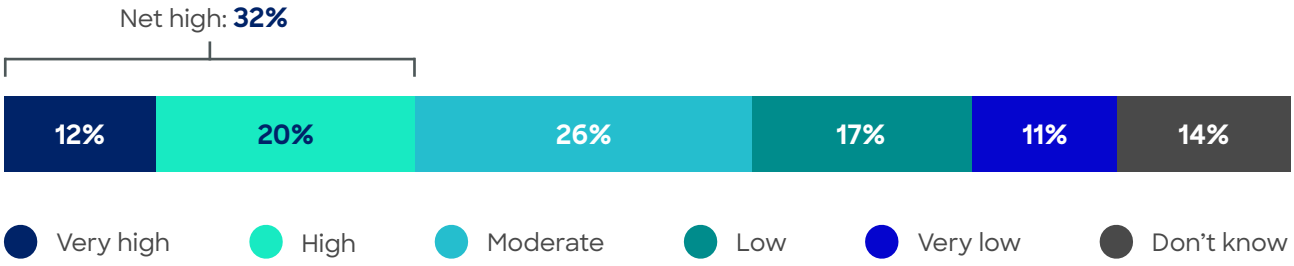
Respondents were also asked whether their own organization has been the victim of a ransomware attack, and if so whether it was successful. Just under a quarter stated that they have been attacked, with 9% having been attacked successfully.

ACAMS Observations

While ransomware is viewed as a current and growing threat by the vast majority of respondents, only a small minority view it as the greatest current cyber threat facing their organization. Additionally, nearly one in ten respondents work at organizations which have been the victim of a successful ransomware attack – while this may be indicative of respondent bias, with victims being more likely to undertake the survey, it certainly demonstrates the widespread nature of the problem.

A third of respondents think the current threat of a ransomware attack on their organization is high.

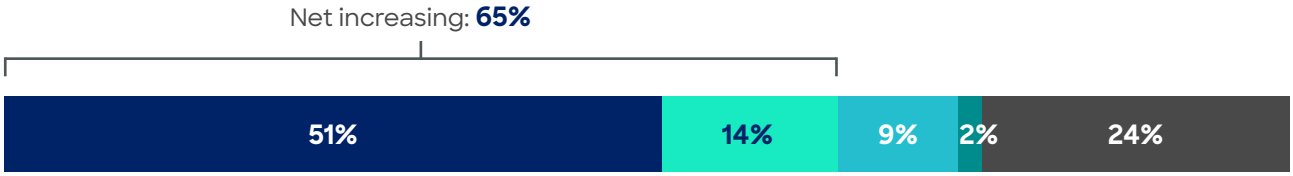
How would you characterize the current threat of a ransomware attack on your organization?



Base: all respondents (395)

Just under two third of respondents think the threat of a ransomware attack on their organization has increased in the past 12 months.

How has your organization's view on ransomware attacks evolved over the past 12 months?



- Ransomware is increasingly seen as a growing threat and a cybersecurity priority
- Ransomware is increasingly seen as a growing threat but not a priority
- The organization's stance on ransomware remains unchanged over the past 12 months
- Ransomware is seen as a diminishing threat
- Don't know

Base: all respondents (395)

Under a tenth of respondents say ransomware is the single greatest cyber-threat their organization faces, and half say it is a high priority.

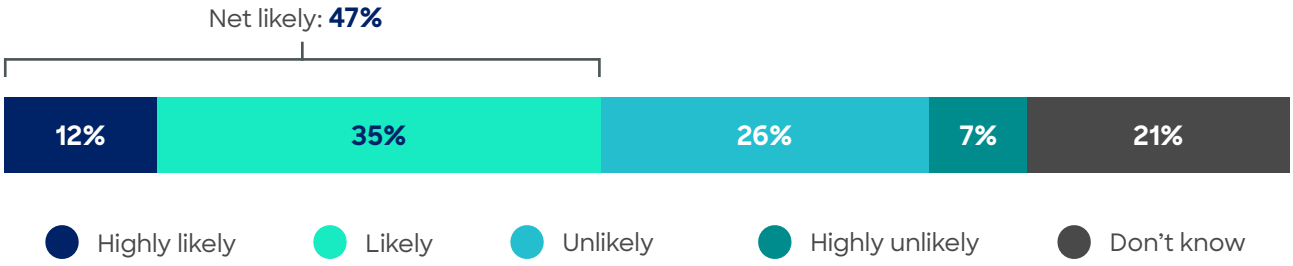
How does the threat of a ransomware attack compare with other cyber-threats to your organization?

- Ransomware is the greatest cyber-threat the organization faces
- Ransomware is one of several high-priority cyber-threats
- Ransomware is a moderate cyber-threat to the organization
- Ransomware attacks are a minor concern compared to other cyber-threats
- Don't know

Base: all respondents (395)

Almost half of respondents think it likely that their organization will be the target of a ransomware attack in the next 12 months.

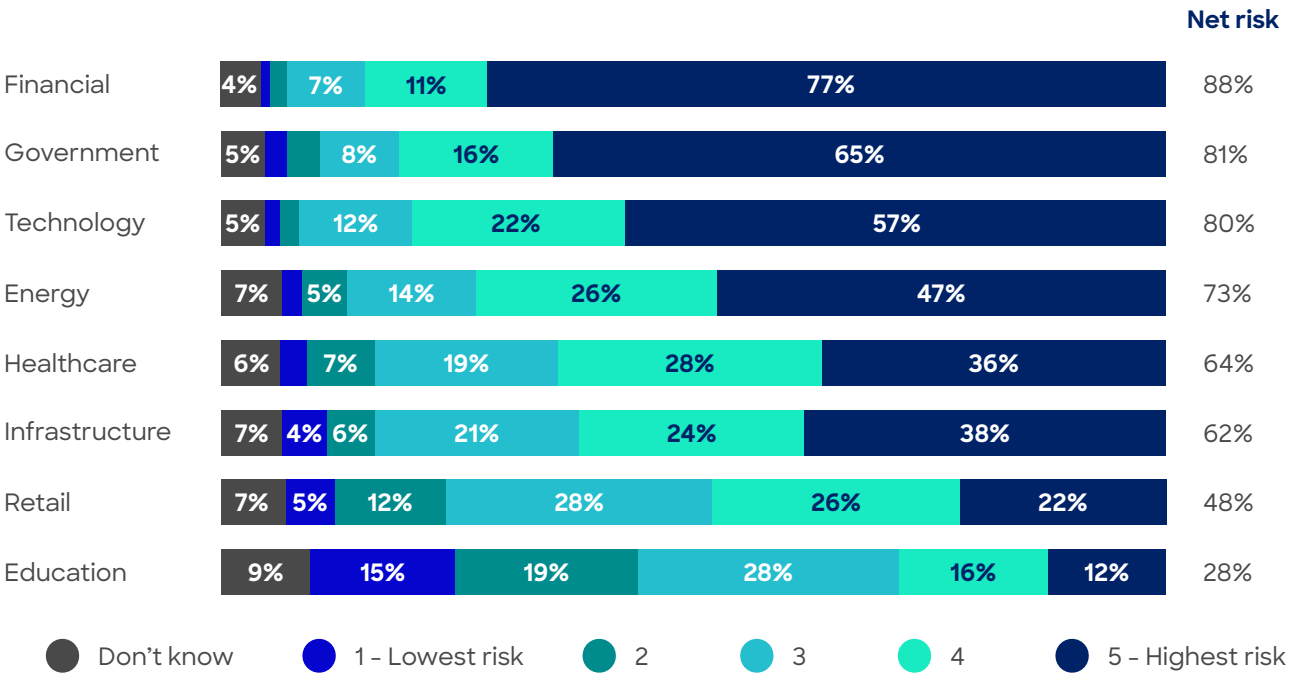
In your opinion, what is the likelihood that your organization will be the target of a ransomware attack in the next 12 months?



Base: all respondents (395)

Finance, government, and tech are the sectors most at risk of ransomware attacks according to respondents.

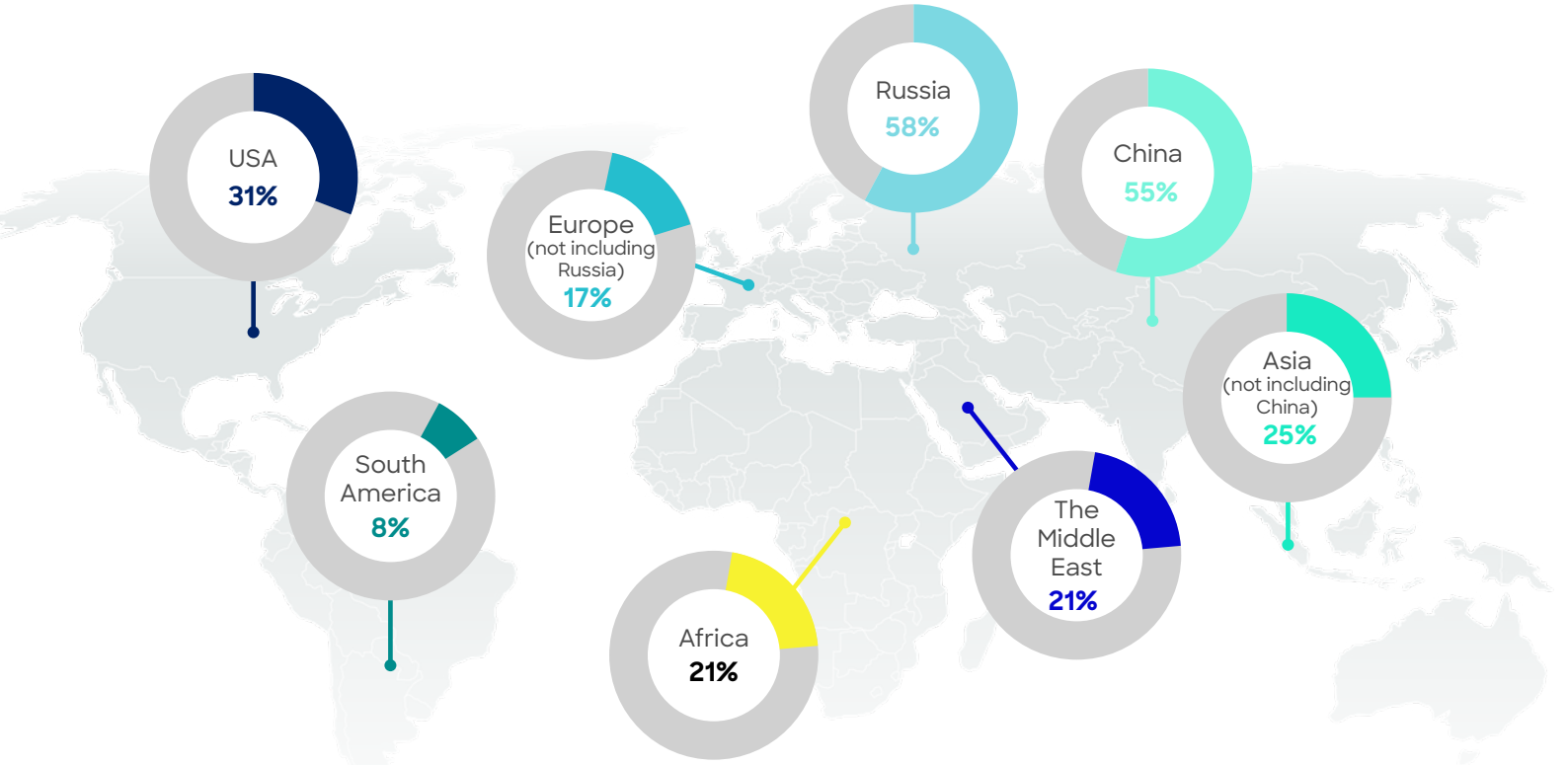
To what extent, if at all, do you think each of the following sectors are at risk of ransomware attacks?



Base: all respondents (395)

Russia and China are seen as the most likely origin point of ransomware attacks.

Which jurisdictions or regions do you think are the most likely to be the origin point of ransomware attacks?



Other - **3%**
Don't know - **11%**

Base: all non-government respondents (395). Respondents were asked to select up to three answers.

Just under a quarter of industry respondents are aware they have been targeted by a ransomware attack; for almost one in ten it was successful.

Has your organization been the target of a ransomware attack?

- Yes, we have been attacked both successfully and unsuccessfully
- Yes, and it was successful
- Yes, but it was unsuccessful
- No
- Don't know

Base: all non-government respondents (348)

Awareness of Ransomware Sanctions Risks and Obligations

This survey sought to understand the extent to which industry, particularly those working in compliance, are familiar with the sanctions risks that ransomware payments can pose, as well as the relating legal obligations.

Non-FI respondents were asked whether they had a sanctions compliance program. Those who answered yes were then asked whether ransomware sanctions risks are considered within that program, with 38% answering yes, and 34% answering no. FI respondents were also asked the same question, with 42% answering yes, and 23% answering no.

Respondents were also asked about their familiarity with the sanctions risks posed from making ransomware payments. Non-FI respondents answered 28% that they were familiar, while 44% were either not at all familiar or quite unfamiliar. By comparison, 24% of FI respondents were familiar, and 50% unfamiliar. Accordingly, respondents were on the whole unfamiliar with ransomware sanctions risks.

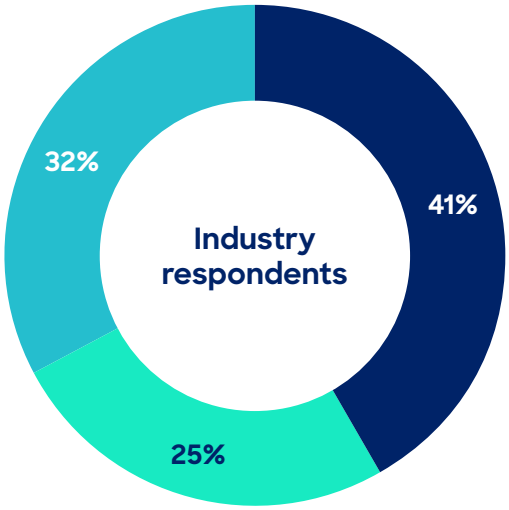
Respondents were also asked their familiarity with the Office of Foreign Assets Control (OFAC) and the Financial Crimes Enforcement Network (FinCEN) ransomware advisories. It should be kept in mind that these are advisories issued by US government agencies. FIs and non-FIs were broadly similar in their familiarity with OFAC and FinCEN ransomware advisories, being between 27-30% net familiarity and between 52-55% net unfamiliarity.

ACAMS Observations

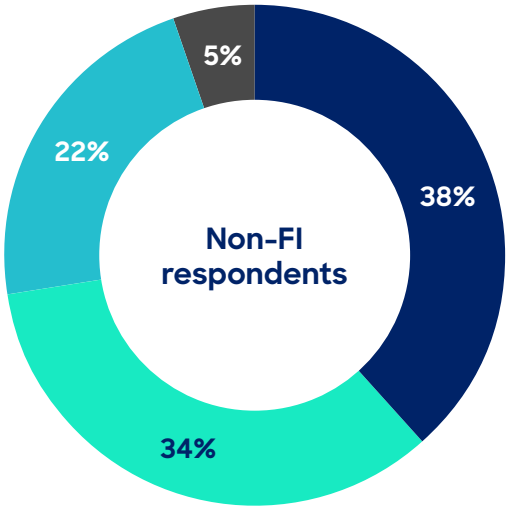
Ransomware is, for many in the sanctions compliance community, still a relatively new area, and this survey indicates that many are not factoring ransomware sanctions risks into their SCP. Large segments of both FI and non-FI respondents are unfamiliar with the potential sanctions risks that can result from ransomware payments and, perhaps surprisingly, non-FI respondents consider themselves to be marginally more familiar with these risks than FI respondents. There is also a significant lack of familiarity with the OFAC and FinCEN ransomware advisories; while these are US government advisories, they provide typologies and useful best practices which apply regardless of jurisdiction.

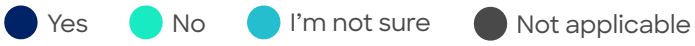
Under half of industry respondents consider ransomware sanctions risks within their sanctions compliance program.

Are ransomware sanctions risks considered within the context of your organization's sanctions compliance program?

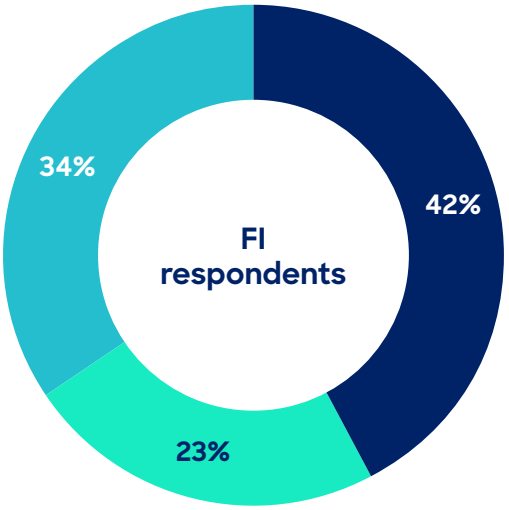


Base: industry respondents with a sanctions compliance program (311)





Base: all non-financial institution respondents with a sanctions compliance program (58)

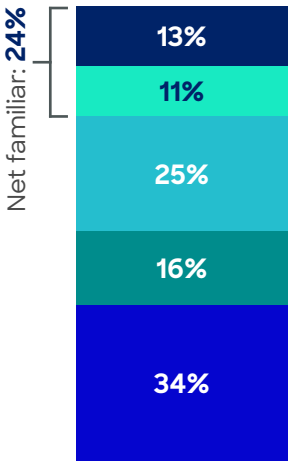


Base: all financial institution respondents with a sanctions compliance program (253)

A quarter of FI respondents and just over a quarter of non-FI respondents are familiar with the sanctions risks associated in making ransomware payments to cyber criminals.

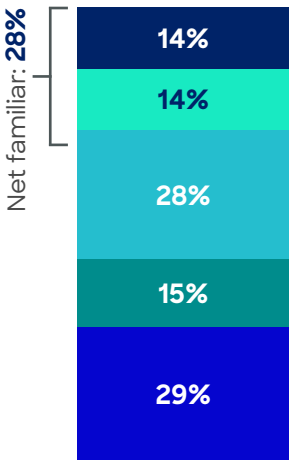
How familiar are you with the sanctions risks associated in making ransomware payments to cyber criminals?

FI respondents



Base: all financial institution respondents (253)

Non-FI respondents



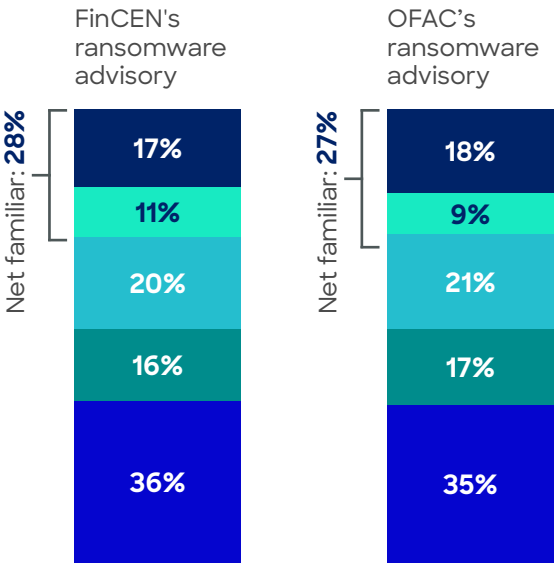
Base: all non-financial institution respondents (95)

1 - Not at all familiar | 2 | 3 | 4 | 5 - Very familiar

Over a quarter of FI respondents and at least a quarter of non-FI respondents are aware of either FinCEN's or OFAC's ransomware advisory.

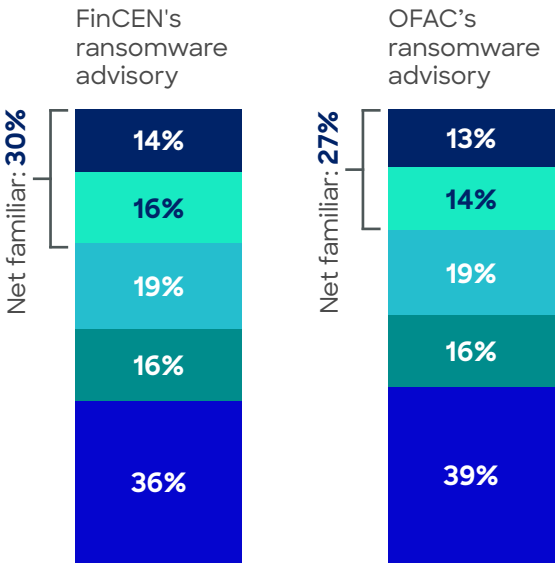
To what extent, if at all, are you familiar with each of the following?

FI respondents



Base: all financial institution respondents (253)

Non-FI respondents



Base: all non-financial institution respondents (95)

1 - Not at all familiar | 2 | 3 | 4 | 5 - Very familiar

Protection Against Ransomware

The survey asked respondents questions about the protection and processes in place for managing a ransomware attack.

Only 5% of respondents felt that their organization is inadequately protected from ransomware attacks, with 40% believing it is strongly shielded. 44% felt there was some level of protection but more could be done.

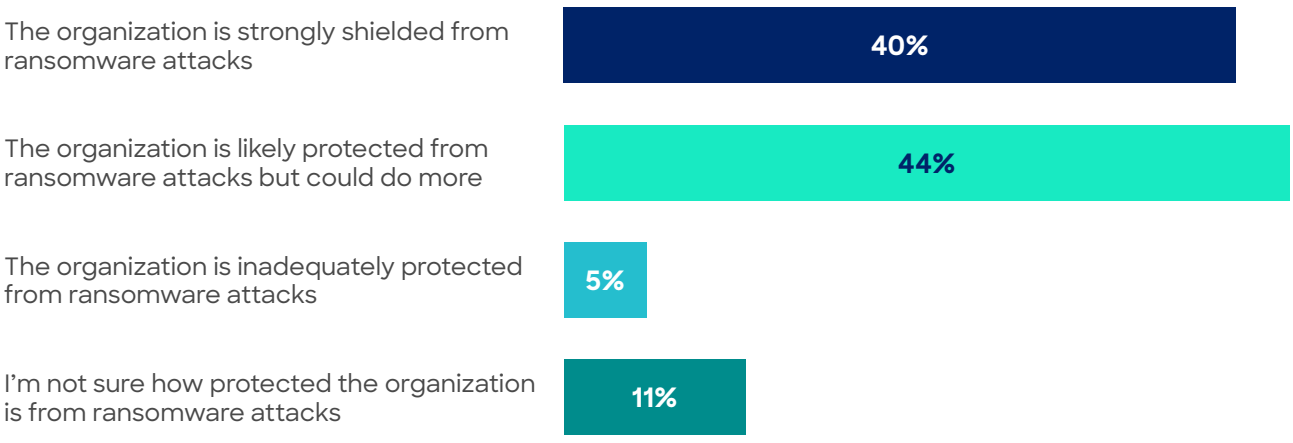
61% stated that their organization has taken more steps to protect itself from ransomware attacks over the past 12 months, in contrast to only 7% stating that it had not. 58% of respondents have a cyber incident response plan in place, and 12% do not. Of those with a cyber incident response plan, an overwhelming majority believe it is effective (81%), with just over half of those classifying it as very effective. Only 2% felt it was ineffective.

ACAMS Observations

A cornerstone of mitigating ransomware sanctions risks is having processes and procedures in place that not only shield an organization from an attack in the first place, but also provide an incident response plan in the event of an attack. Reflecting the belief that ransomware is a growing threat – as indicated earlier in this report – most respondents' organizations have taken further steps to protect themselves in the past year. The majority of respondents felt that their organization has some level of protection, with nearly half believing they are strongly shielded. Of those who have a cyber incident response plan, the majority view it as effective in mitigating the ransomware threat.

Four in ten industry respondents say their organization is strongly shielded from ransomware attacks, but almost half say they could do more.

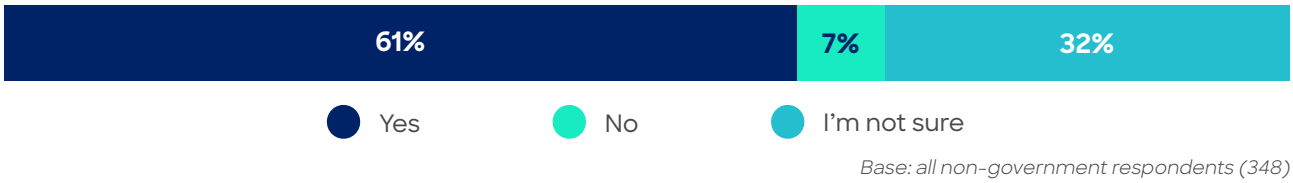
Which of the following statements best describes the maturity of cyber security controls at your organization?



Base: all non-government respondents (348)

Almost two-thirds of industry respondents say their organization has taken steps over the past 12 months to protect itself from ransomware attacks.

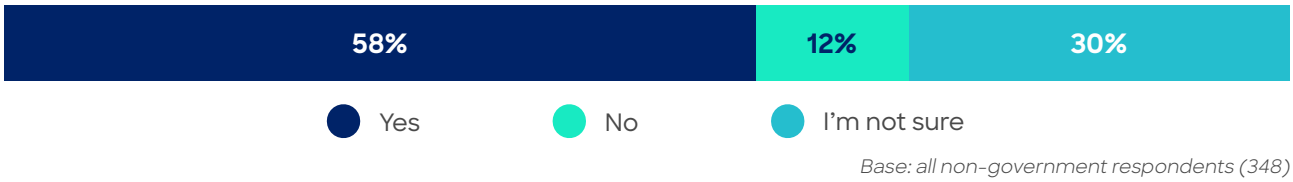
Has your organization taken additional steps over the past 12 months to protect itself from ransomware attacks?



Base: all non-government respondents (348)

Over half of industry respondents believe their organization has a cyber incident response plan for ransomware attacks.

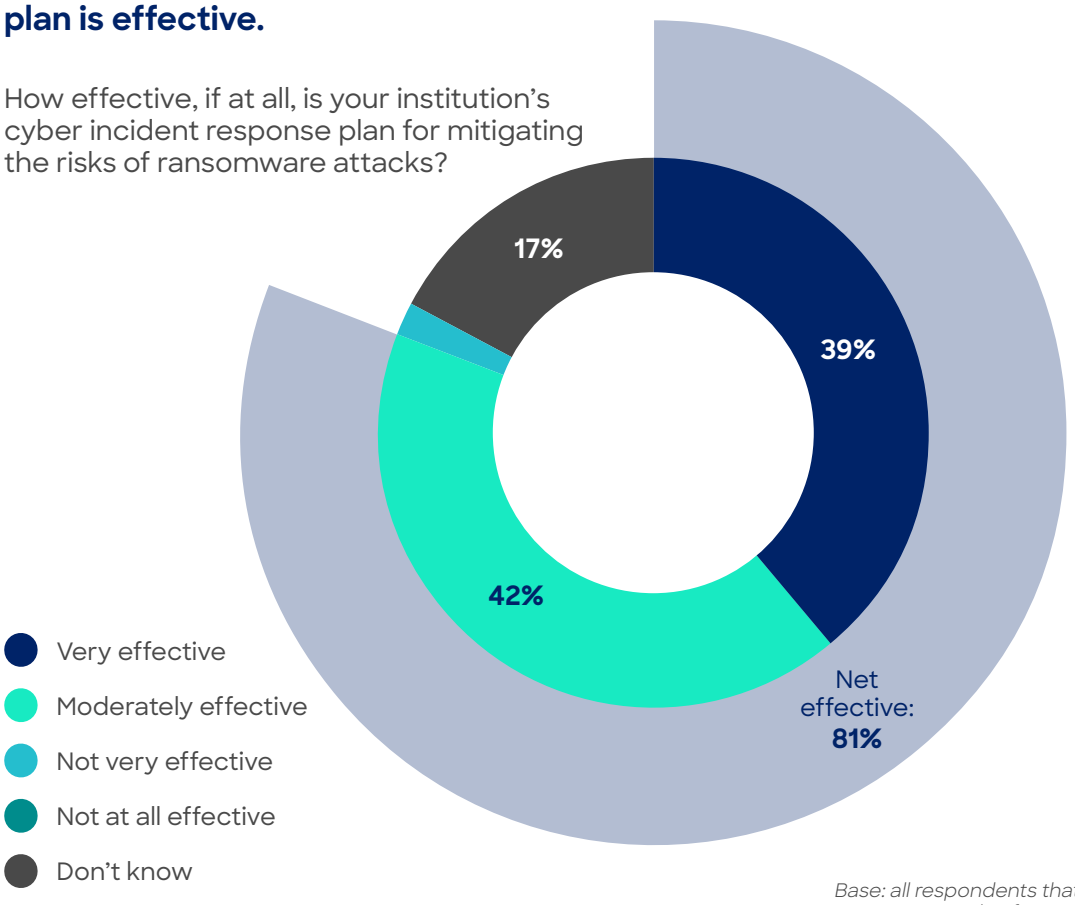
Does your organization have a cyber incident response plan for ransomware attacks?



Base: all non-government respondents (348)

More than eight out of ten respondents believe their cyber incident response plan is effective.

How effective, if at all, is your institution's cyber incident response plan for mitigating the risks of ransomware attacks?



Base: all respondents that have a cyber incident response plan for ransomware attacks (201)

Sanctions Compliance and AFC Governance

When asked about the specific policies and procedures in place to mitigate the financial crime risks of ransomware, answers diverged significantly between FI and non-FI respondents. Among FIs, most respondents (40%) were not aware whether they had a risk-appetite statement on ransomware sanctions compliance, with 26% stating yes and 34% no. In comparison, while 29% of non-FI respondents didn't know, 54% stated they did not have a risk-appetite statement on ransomware sanctions compliance, with 17% answering that they did.

Respondents were further asked which stakeholder groups are required to participate as part of their organization's cyber incident response plan, with the results indicating that in many cases anti-financial crime personnel are not involved – with 58% including AML, 50% including anti-fraud, and only 40% including sanctions compliance professionals. Sanctions professionals are only involved in identifying and investigating ransomware attacks for 53% of respondents.

Just over half of respondents have an incident response plan for ransomware attacks, and under half have policies and procedures for ransomware-related risk-management (48%), anti-financial crime training which addresses ransomware (42%), and other training which addresses ransomware risks (47%). When breaking this down by sector, FI respondents were on average nearly 10% more likely to have the above than non-FI respondents.

Furthermore, only 24% of respondents are aware of a process/threshold to determine when a potential ransomware attack should be elevated to the anti-financial crime compliance department, and only 53% are aware of the terms of their ransomware insurance (if they have any) and what measures need to be taken to comply with it.

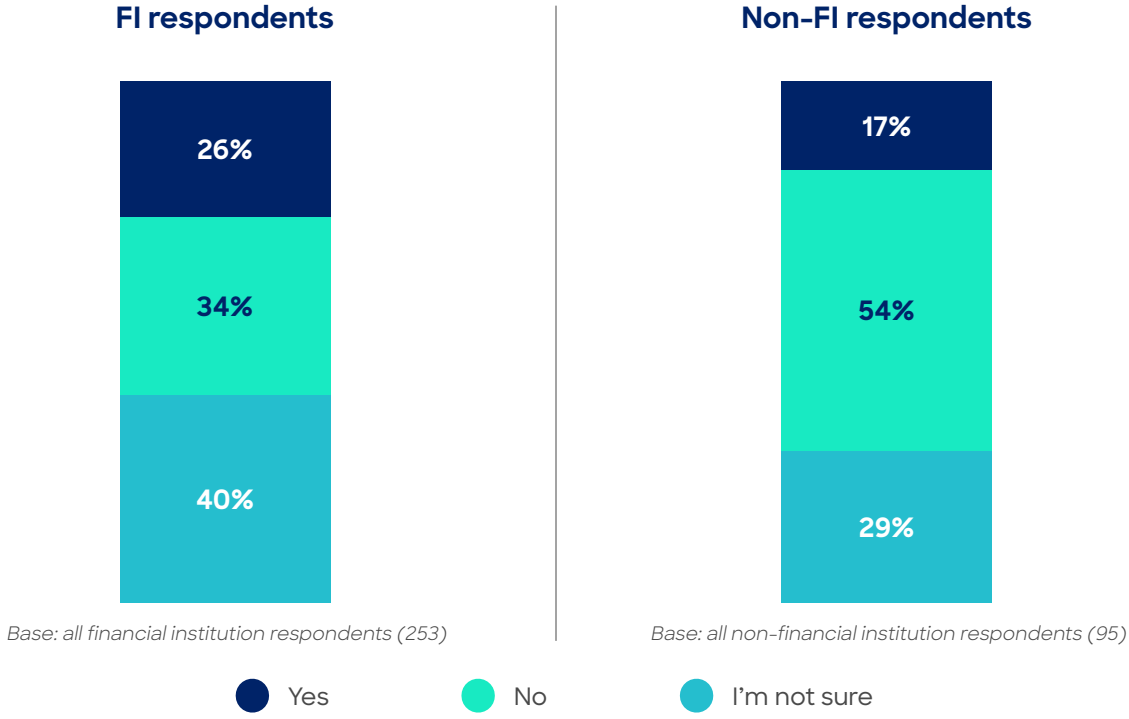
ACAMS Observations

When asked about the anti-financial crime protections against ransomware attacks, respondents were generally divided on most aspects, including actual participation of anti-financial crime teams in ransomware response plans and investigations. Sanctions compliance ranked the lowest of these, further emphasizing a lack of understanding of ransomware sanctions risks as outlined earlier in this report.

When asked about specific policies, procedures, and training on ransomware, roughly half of respondents stated that they have these. It should be noted that a significant portion responded that they weren't sure, which does not mean that those organizations do not have these processes, just that the respondent is unaware of them. Nevertheless, a fair percentage stated that they do not have AFC training addressing ransomware or related risk management policies and procedures.

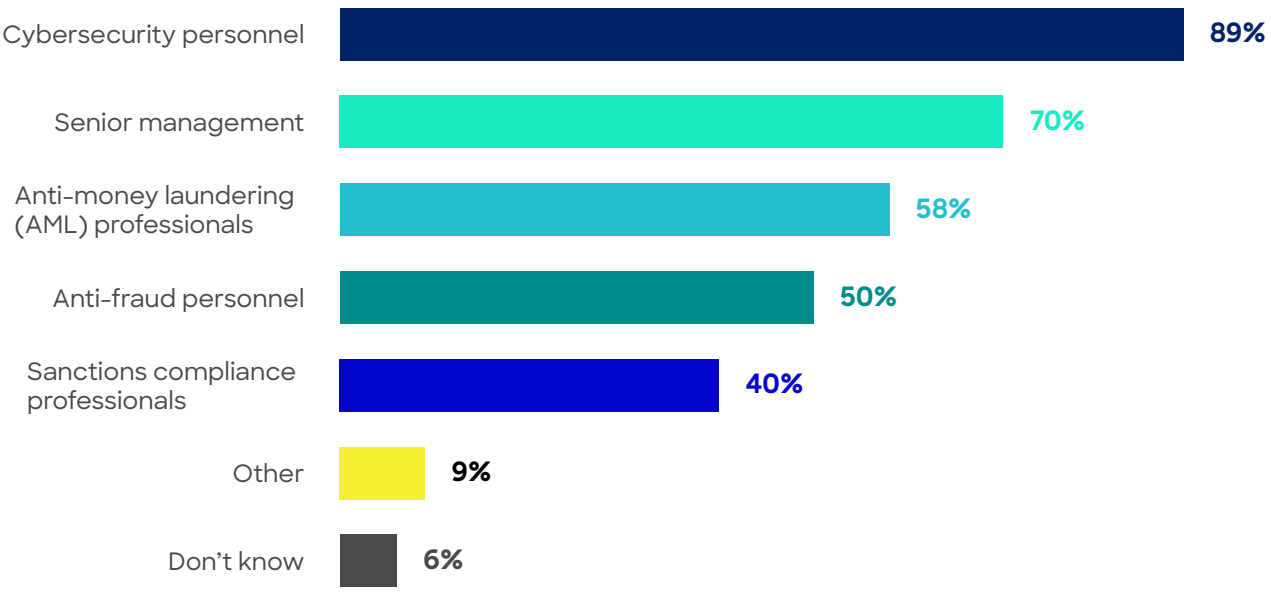
Over a third of FI respondents organizations and over half of non-FI respondents organizations have not drafted a risk-appetite statement on ransomware sanctions compliance.

Has your organization drafted a risk-appetite statement on ransomware sanctions compliance?



Less than half of respondents require the participation of sanctions compliance professions within their incident response plan.

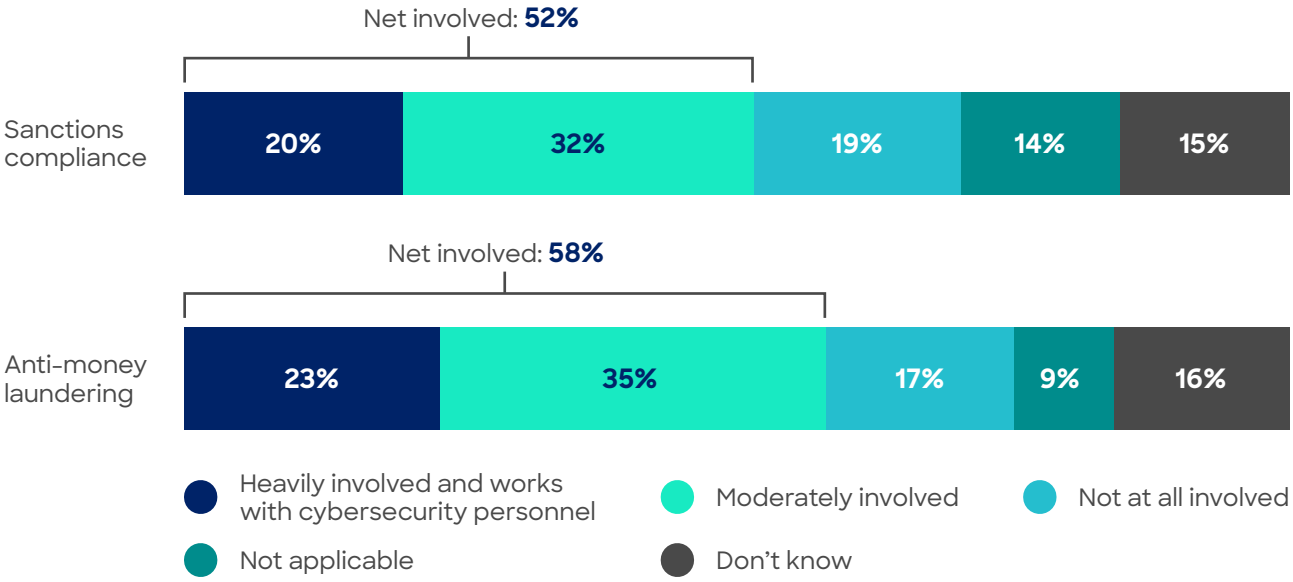
From which of the following stakeholder groups, if any, is participation required as part of your organization's cyber incident response plan?



Base: all respondents that have a cyber incident response plan for ransomware attacks (201)

Over half of industry respondents say both sanctions compliance and anti-money laundering teams are involved in identifying and investigating ransomware attacks.

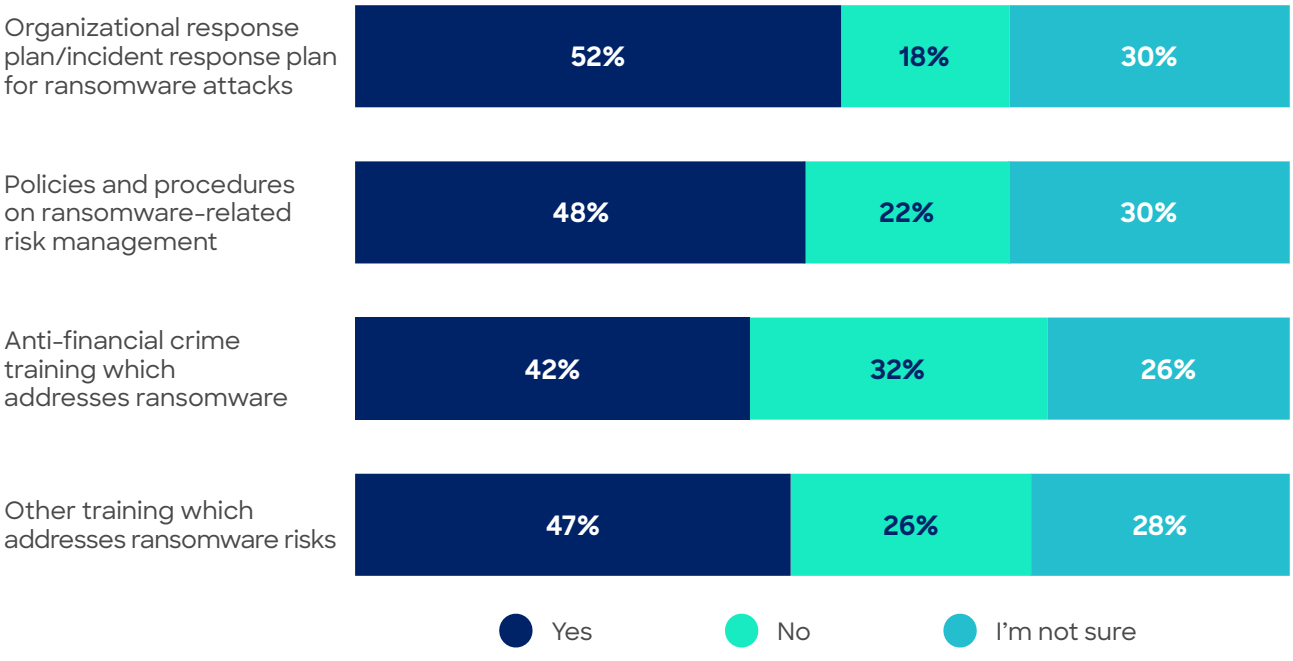
To what extent, if at all, are the following teams in your organization involved in identifying and investigating ransomware attacks?



Base: all non-government respondents (348)

Approximately half of respondents have ransomware-related policies, procedures and training.

When thinking about its approach to ransomware attacks, does your organization have the following?

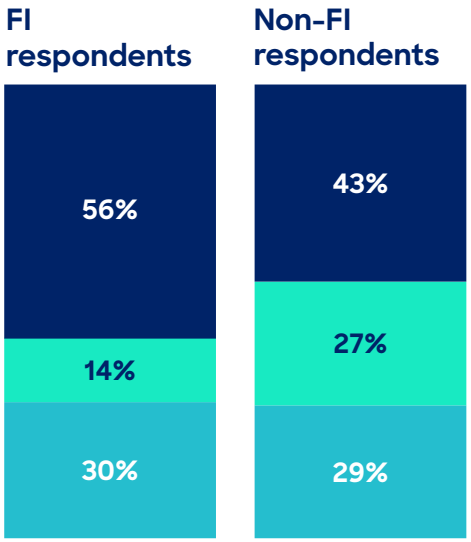


Base: all non-government respondents (348)

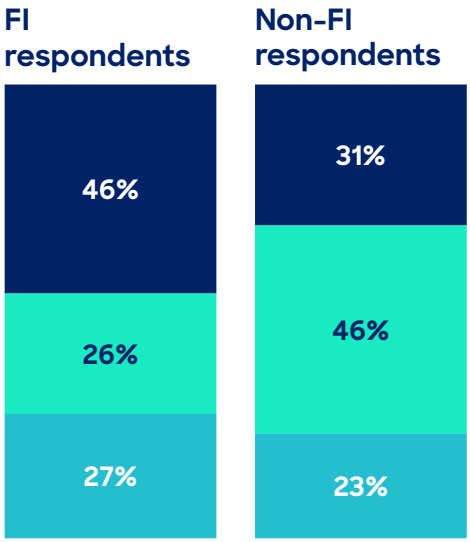
Over half of FI respondents have organizational response plans for ransomware attacks and policies on ransomware-related risk management, and under a third of non-FI respondents have specific anti-financial crime training which addresses ransomware.

When thinking about its approach to ransomware attacks, does your organization have any of the following?

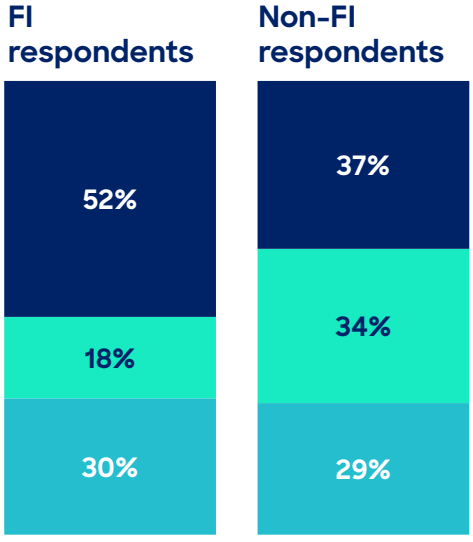
Organizational response plan/ incident response plan for ransomware attacks



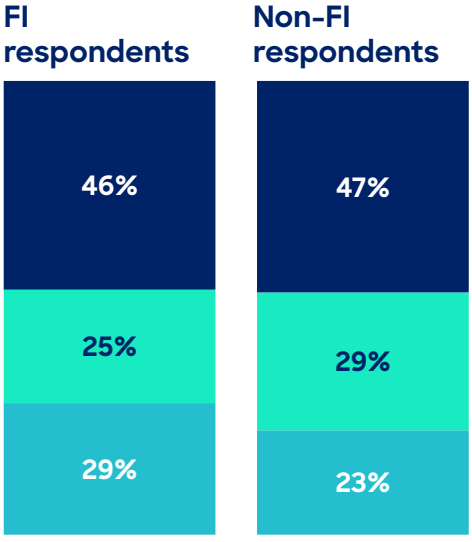
Anti-financial crime training which addresses ransomware



Policies and procedures on ransomware-related risk management



Other training which addresses ransomware risks

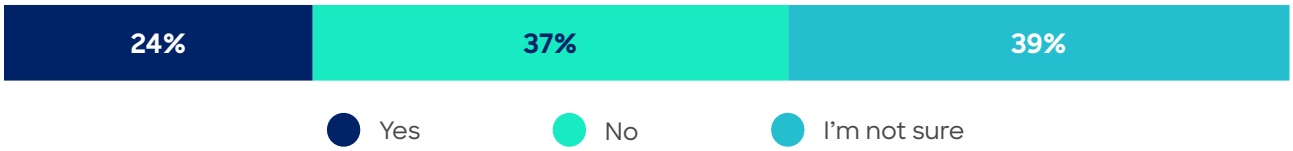


Yes No I'm not sure

Base: all financial institution respondents (253) and all non-financial institution respondents (95)

Just under a quarter of industry respondents have developed a process or threshold for elevating a ransomware attack to the AFC department.

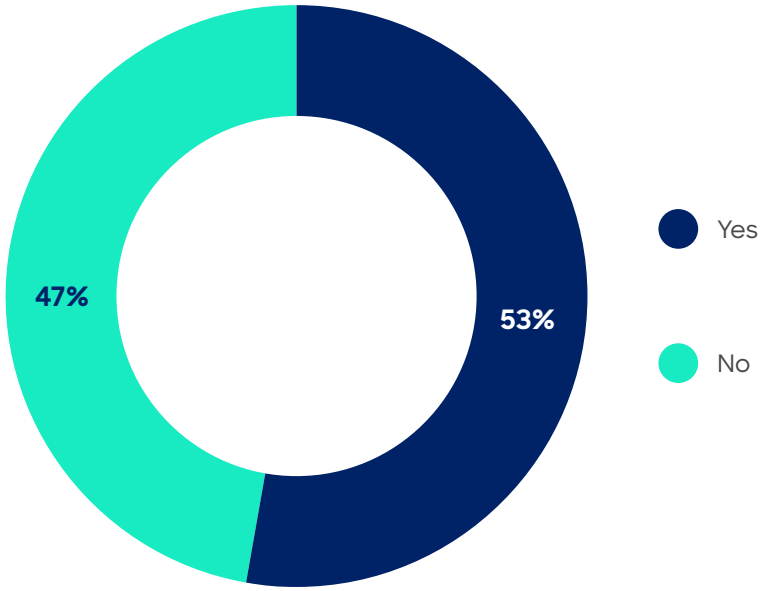
Have you developed a process/threshold to determine when a potential ransomware attack should be elevated to the anti-financial crime compliance department?



Base: all non-government respondents (348)

Just over half of industry respondents with ransomware insurance understand how to comply with it.

Are you aware of the terms of your ransomware insurance and what measures need to be taken to comply with it?



Base: all non-government respondents with ransomware insurance coverage (62)

Enhancing the Global Fight Against Ransomware

The survey sought to understand perceptions around action to be undertaken to enhance the global fight against ransomware. When asked about their national government's efforts on combating ransomware, 29% felt their government had done very little to protect businesses from ransomware attacks. 38% answered that some steps had been taken but much more is needed, 15% stated that an adequate job was being done, and 5% stated an exceptional job had been undertaken.

When asked about government outreach on how to report and respond to ransomware attacks, 37% of respondents said their government had not undertaken any outreach with the private sector. 30% said that their government had undertaken some outreach, but that guidance has been vague. 13% said officials have clearly explained how to respond to ransomware attacks.

Looking forward, respondents were asked what would be most useful for them in dealing with ransomware attacks. A series of options were given, and respondents were asked to rank each from one to five, with five being very useful. The options selected by the most respondents as being useful were:

1. Greater access to specific information on current and emerging threats (76% useful)
2. The issuance of guidance on how to best prevent ransomware attacks (75% useful)

Respondents were also asked which actions by governments would be most useful in the global fight against ransomware, and presented with a number of options. All five options were seen as useful by the majority of respondents, but the three selected as most useful were:

1. Stronger efforts by governments to identify and penalize ransomware groups (79% useful)
2. Greater flexibility within the public and private sectors to share relevant intelligence (77% useful)
3. Stronger training throughout the private sector on how to shield firms from attacks (77% useful)

Additionally, compliance and red flag indicators of ransomware was identified as the most important training topic, with 85% of respondents classifying it as important, followed by integrating cybersecurity with AFC/sanctions compliance (83%), training on mitigating ransomware-related sanctions risks (82%), and ransomware 101 training (80%).

Finally, respondents are largely split on whether ransomware payments should be banned in all cases, with 28% saying they should and 32% saying they shouldn't.

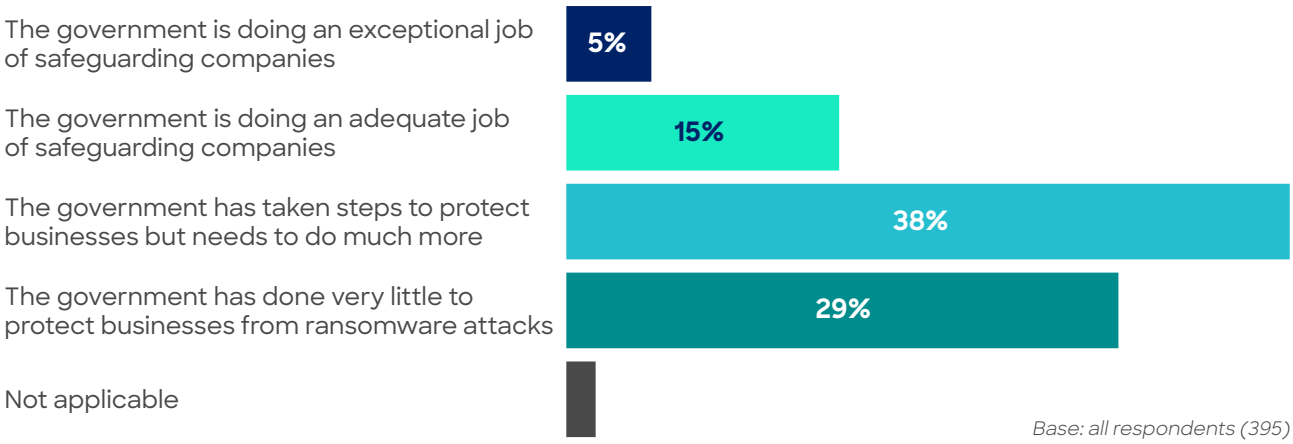
ACAMS Observations

In assessing national governments' efforts to support private industry in dealing with ransomware, the strong majority of respondents feel more needs to be done and, where guidance has been issued, that it is vague. The greatest informational needs identified are a combination of guidance on how to prevent attacks as well as information sharing on emerging threats. Other needs identified by most respondents include stronger training throughout the private sector and greater flexibility for public-private sector information sharing. Respondents believe that stronger efforts by governments to identify and penalize ransomware groups would be the most effective way to advance the global fight against ransomware, with 79% of those surveyed viewing this as useful.

There is ongoing debate across a number of jurisdictions on whether ransomware payments should be outlawed in all cases, and on this issue respondents were unaligned, with roughly a third saying they should, a third saying they should not, and a third not sure.

Over a third of industry respondents say the government needs to do much more to safeguard against ransomware attacks.

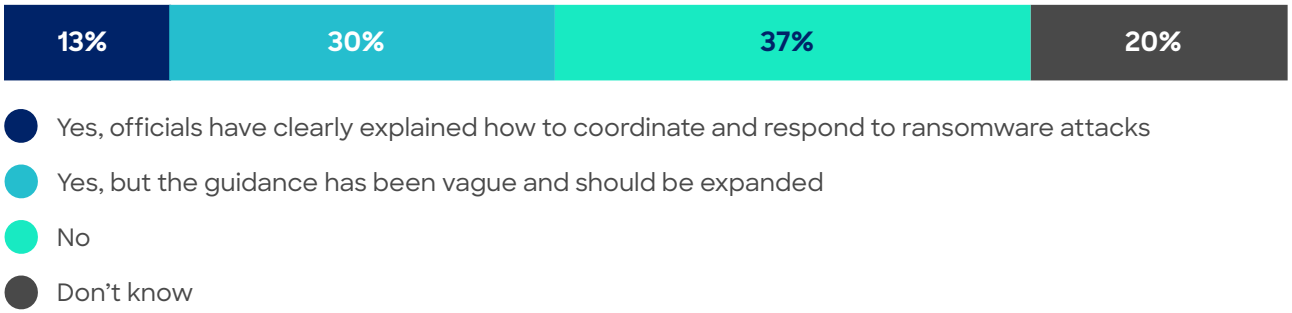
How would you characterize your national government's efforts to provide information/ guidance to private sector organizations to safeguard against ransomware attacks?



Base: all respondents (395)

Almost a third of industry respondents feel that government guidance on ransomware has been vague and should be expanded.

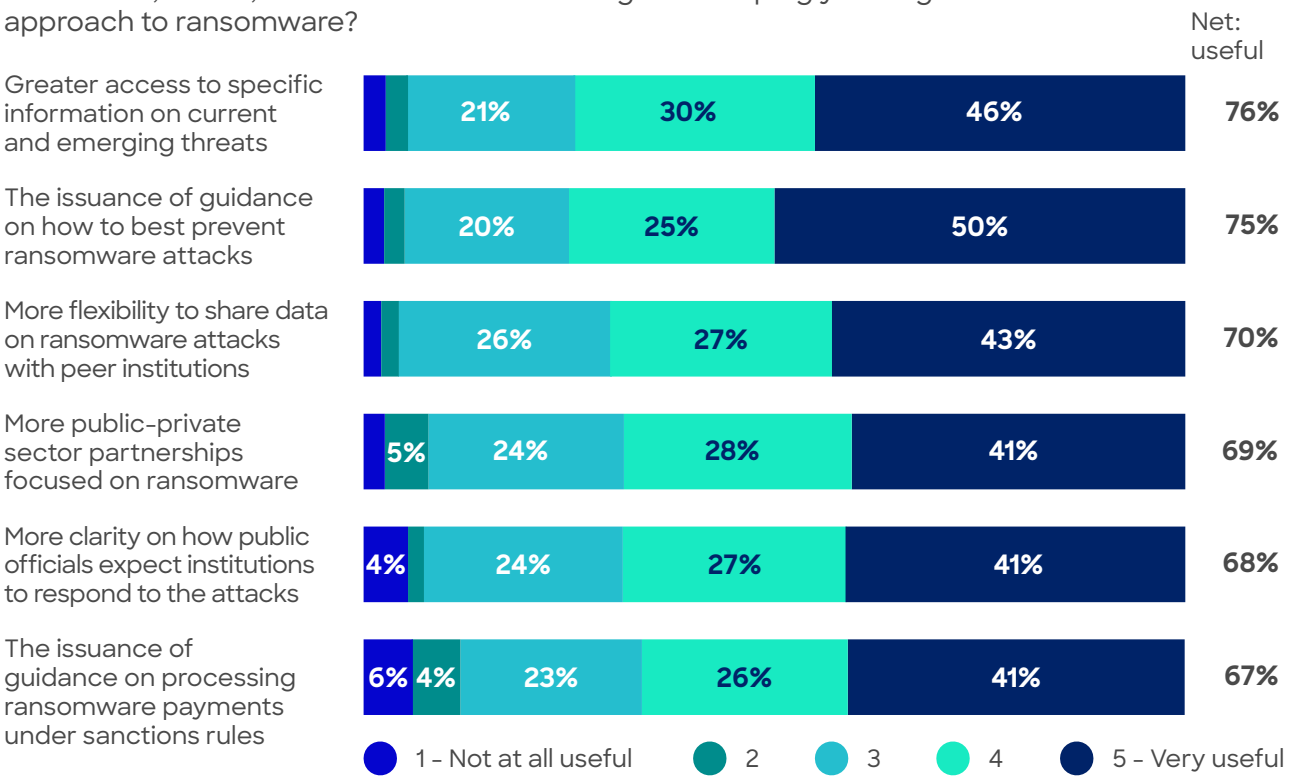
Has your national government conducted any outreach with your organization (or sector at large) on how to report and respond to ransomware attacks?



Base: all non-government respondents (348)

Three quarters of respondents think greater access to specific information on threats and guidance on how to prevent attacks would be helpful to their organization.

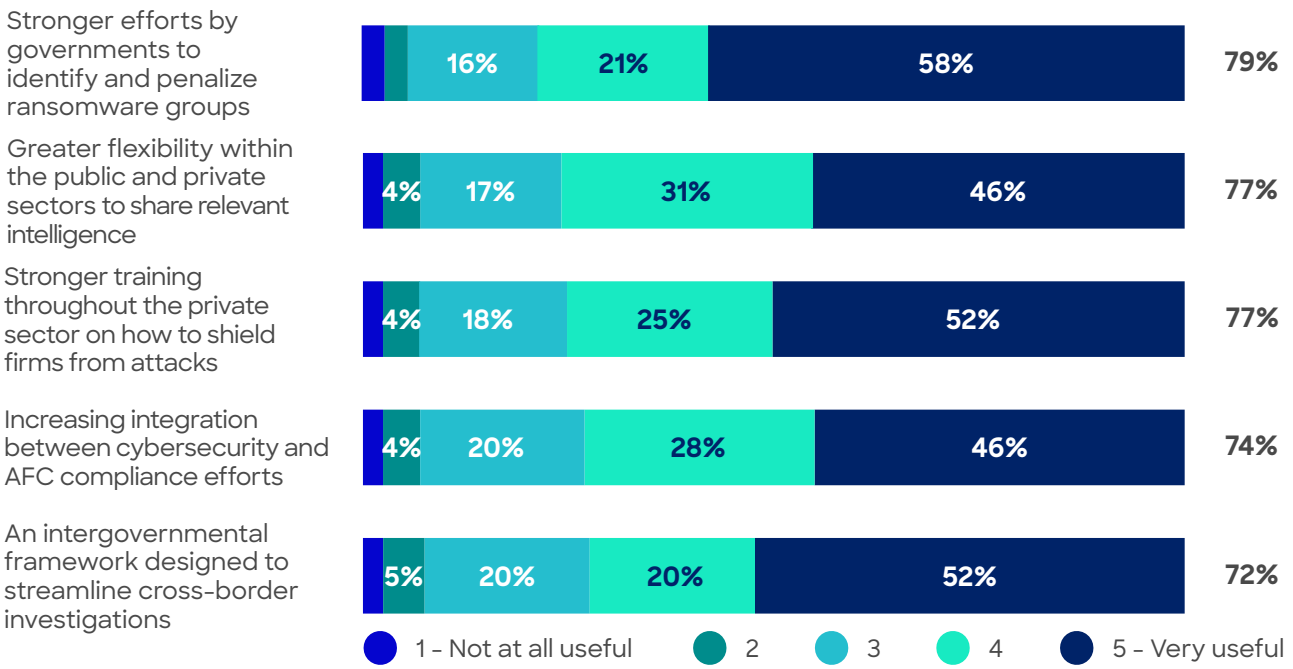
How useful, if at all, would each of the following be in helping your organization's approach to ransomware?



Base: all non-governmental respondents (348)

Industry respondents feel stronger government efforts to identify and penalize ransomware groups would be most helpful in the fight against ransomware.

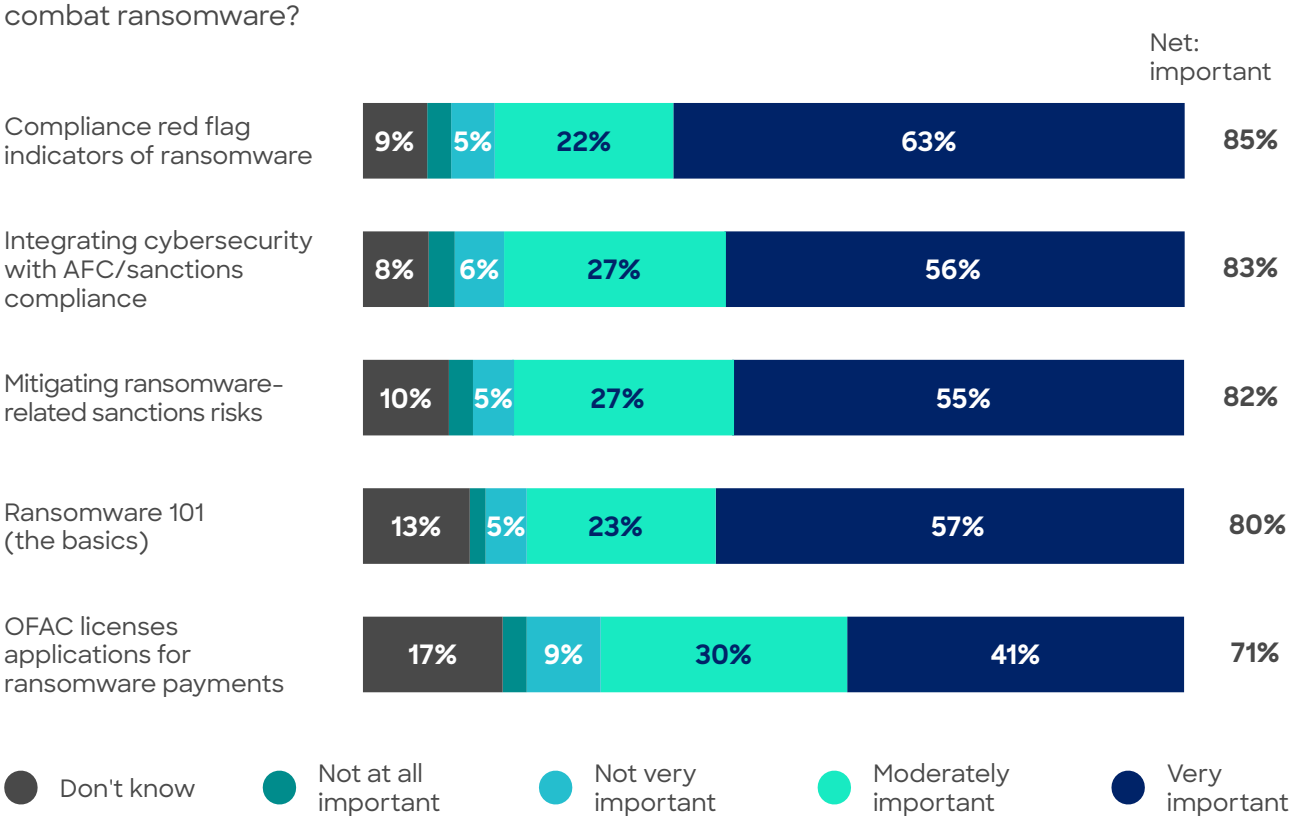
How useful, if at all, would each of the following be in helping the global fight against ransomware?



Base: all respondents (395)

Almost nine out of ten respondents think compliance red flag indicators of ransomware would help the financial sector combat ransomware.

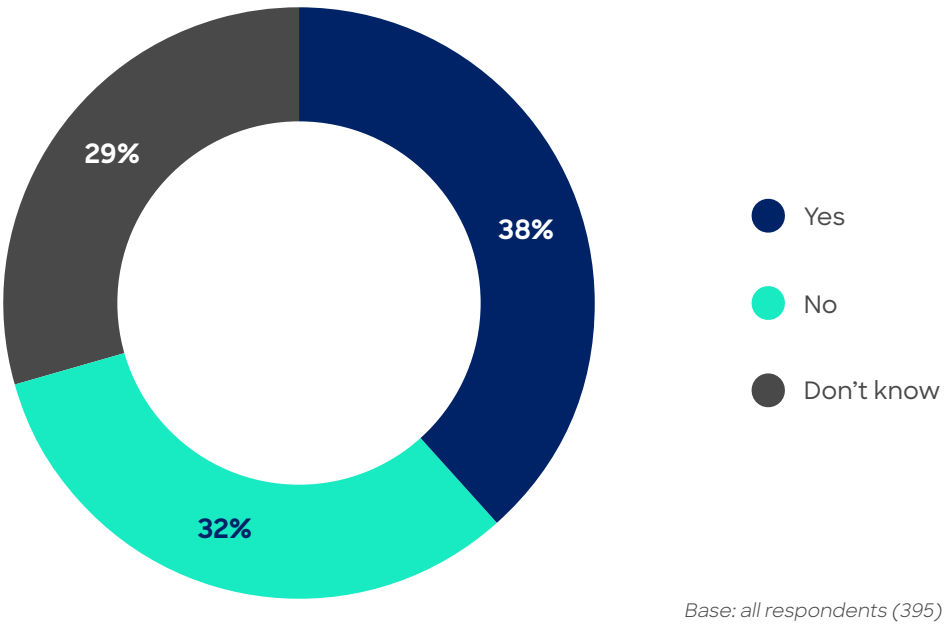
How important, if at all, are each of the following training topics in helping the financial sector combat ransomware?



Base: all respondents (395)

Over a third of respondents think governments should prohibit ransomware payments in all cases.

Should governments prohibit ransomware payments in all cases?



Base: all respondents (395)

Regional Perceptions Breakdown

The survey asked respondents to identify the region in which they are based, and this section will look at the results of the survey through a geographic lens, picking out questions which have already been covered.

When asked about familiarity with ransomware, respondents from the US (55%), Africa (54%), and the Middle East (50%) believed themselves to be the most familiar with ransomware, with Asia (40%) being the lowest. Respondents from the Middle East (92%), Europe (90%), and the USA (86%) believed themselves to be most protected from ransomware.

When asked about the likelihood that they would be targeted by ransomware in the next 12 months, European respondents were by far the most likely to feel they would be attacked, at 63%, with US respondents least likely to say they will be attacked (40%).

In terms of the evolving threat perception of ransomware, US-based respondents were most likely to state that ransomware is seen as a growing threat and a cybersecurity priority (62%), compared with only 48% in Europe and 40% in Asia.

By way of sanctions compliance, respondents from Africa (57%) and the USA (45%) were most likely to include sanctions compliance as part of their organization's cyber incident response plan, and respondents from the Middle East (50%) and the USA (47%) were most likely to consider sanctions risks within the context of their organization's sanctions compliance program. By comparison, only 34% of respondents in both Asia and the Americas (excluding USA) consider sanctions risks within their SCP.

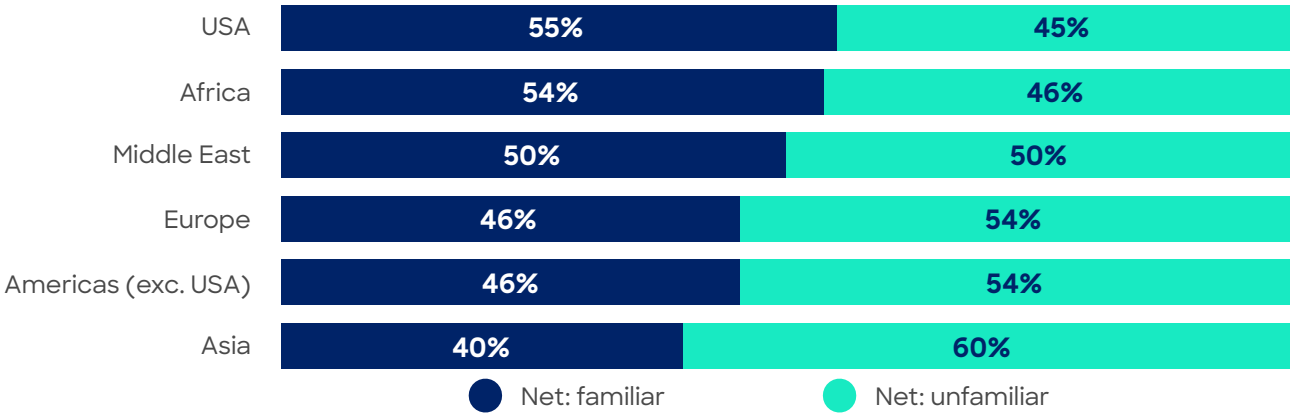
ACAMS Observations

The regional breakdown presents some interesting and at times surprising findings. US respondents, for example, were simultaneously most likely to view ransomware as a growing threat, but least likely to feel they would be attacked in the next 12 months.

The findings outlined here demonstrate that at times, there are distinct regional variations in attitudes towards ransomware across the compliance community.

Respondents based in Africa and the US are most likely to be familiar with ransomware.

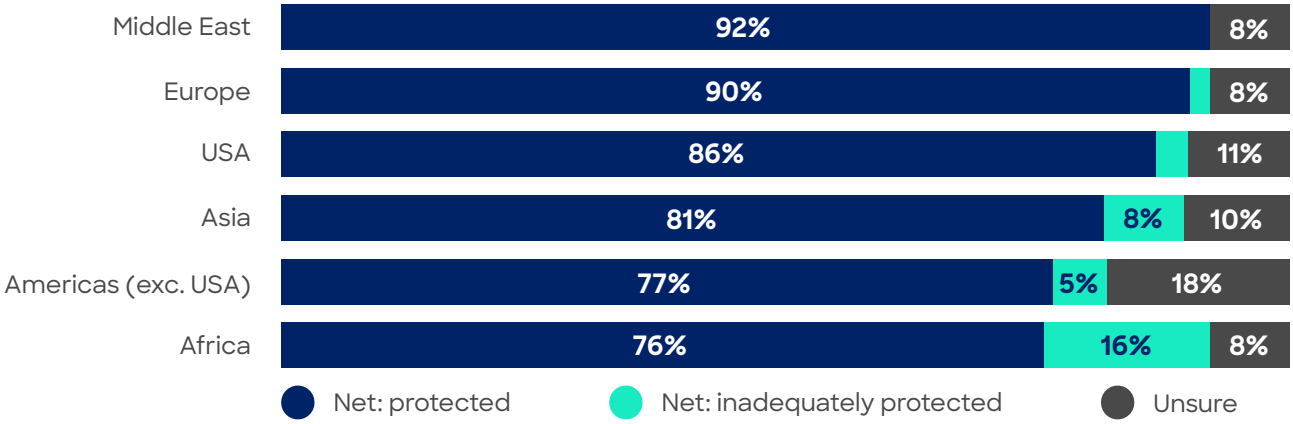
How would you characterize your knowledge of ransomware?



Base: all respondents (395)

Respondents based in Europe and the Middle East are most likely to consider themselves protected from ransomware.

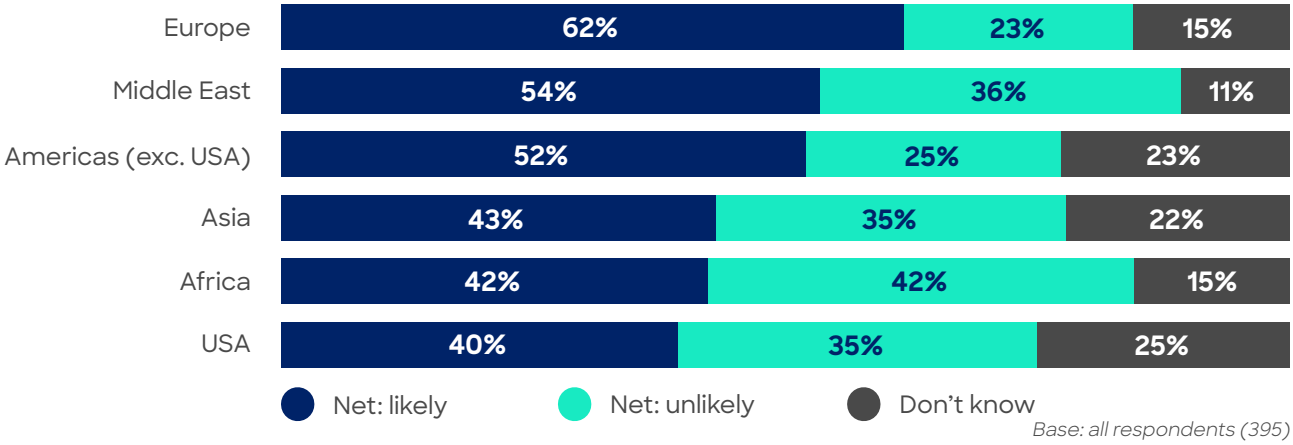
Which of the following statements best describes the maturity of cyber security controls at your organization?



"Protected" combines responses that considered themselves either "strongly shielded" or "likely protected" from ransomware attacks.
Base: all non-government respondents (348)

Respondents based in Europe are by far the most likely to believe they will be the target of a ransomware attack in the next year.

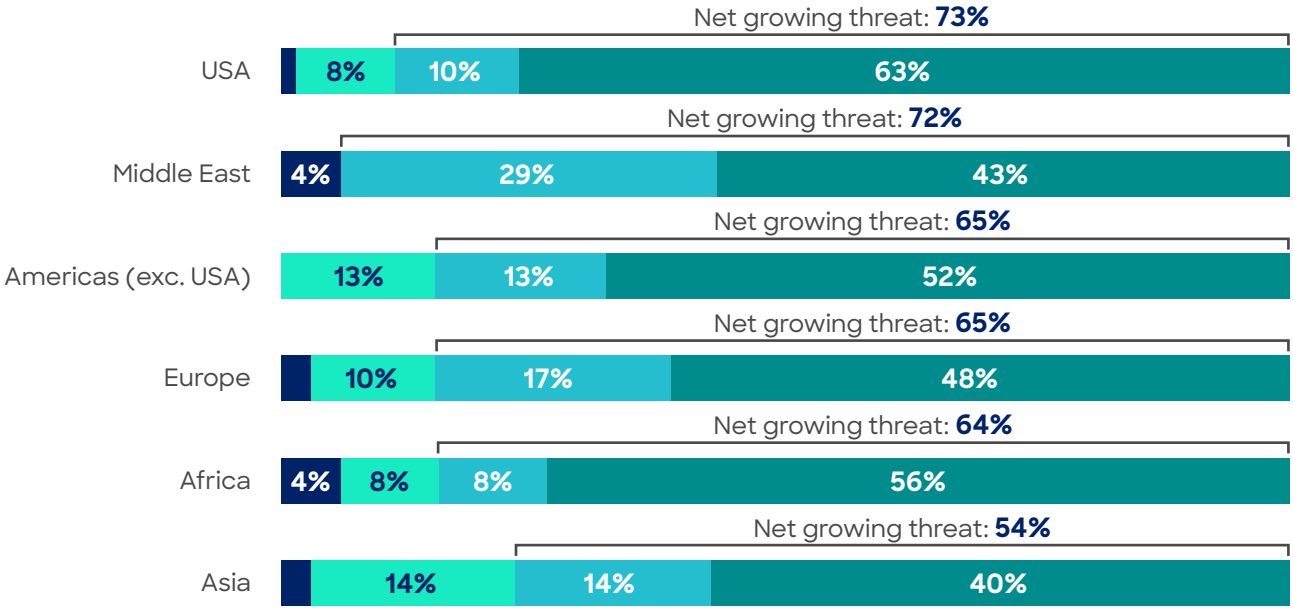
In your opinion, what is the likelihood that your organization will be the target of a ransomware attack in the next 12 months?



Base: all respondents (395)

Respondents in the US are most likely to believe their organization views ransomware as a growing threat.

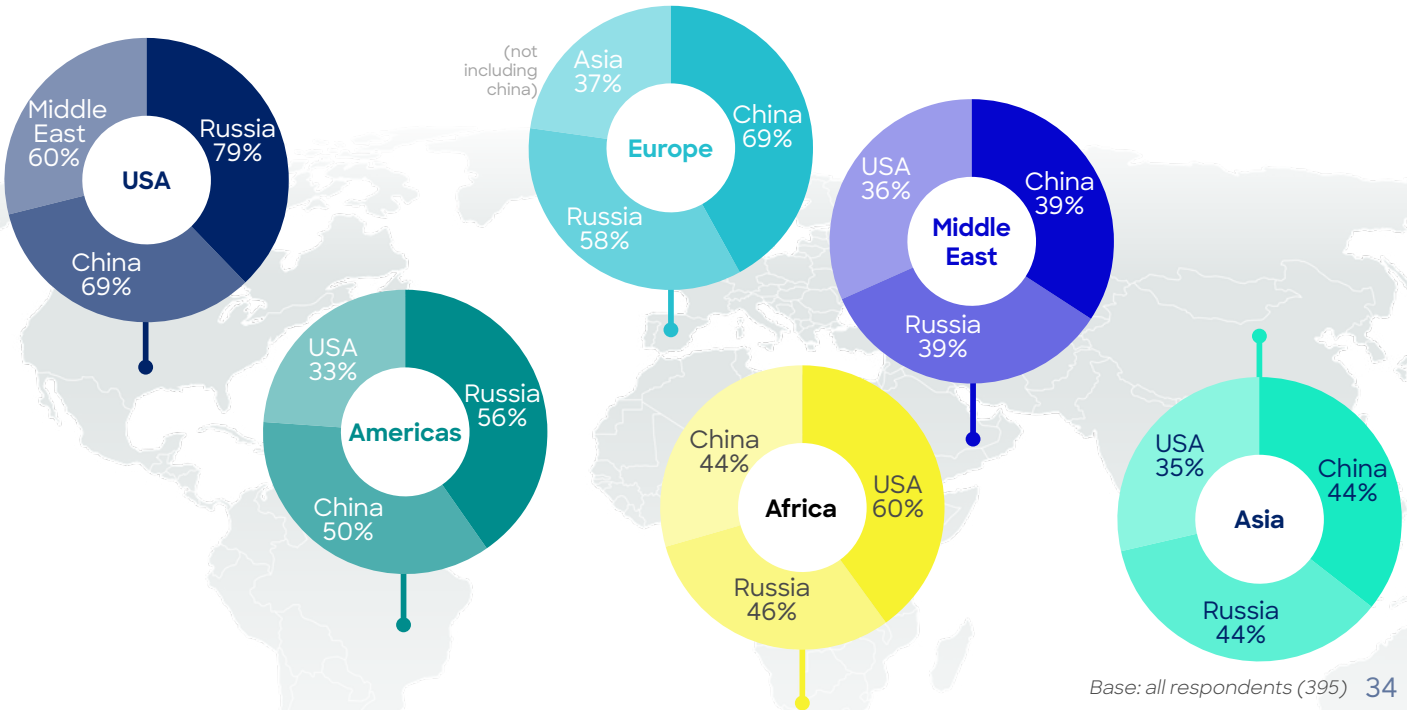
How has your organization's view on ransomware attacks evolved over the past 12 months?



Base: all respondents (395).
Chart excludes 'Don't know' responses.

Respondents in the USA and Europe are most likely to view Russia and China as the most likely origin point of ransomware attacks.

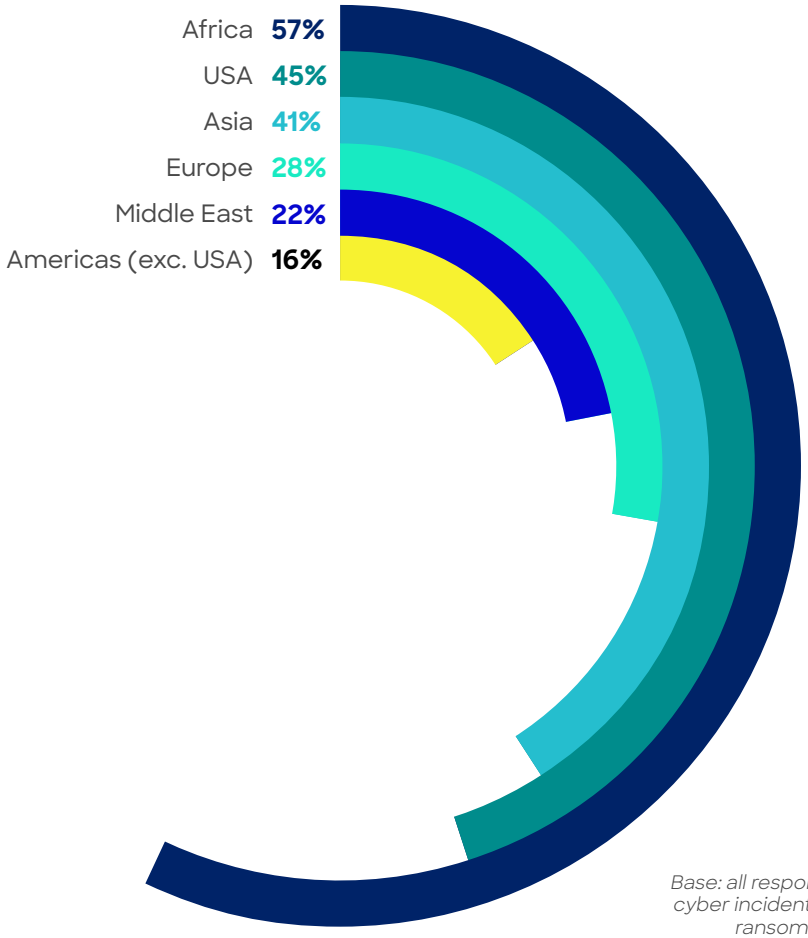
Respondents were asked to select the three jurisdictions most likely to be the origin point of a ransomware attack. The top three for each jurisdiction are:



Base: all respondents (395)

Respondents in Africa and the USA are most likely to include sanctions professionals in their incident response plan.

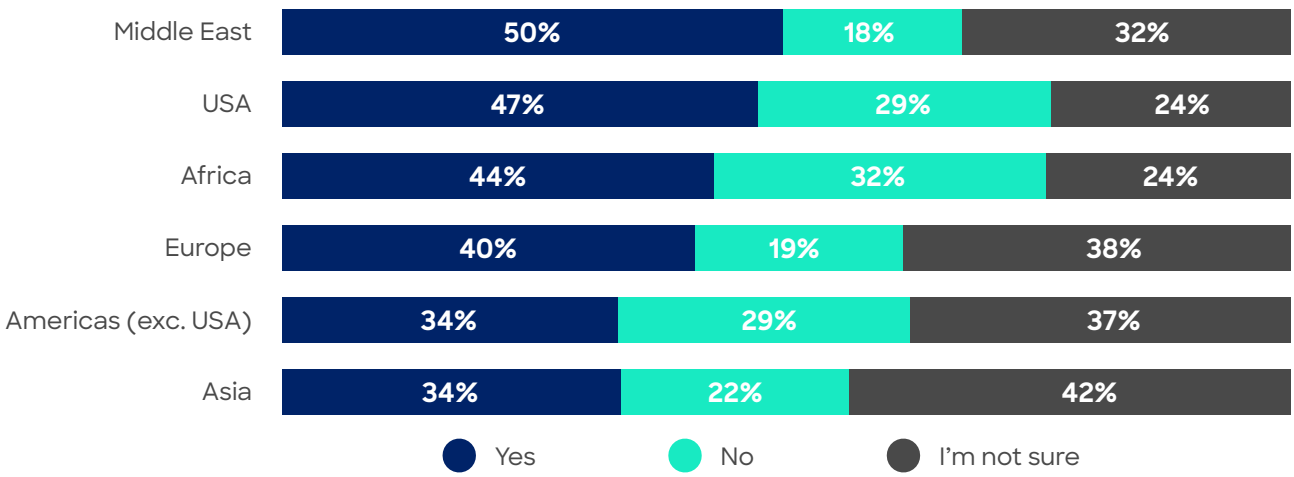
Are sanctions compliance professionals required as part of your organization's cyber incident response plan?



Base: all respondents that have a cyber incident response plan for ransomware attacks (201)

Respondents in Asia and the Americas (exc. USA) are least likely to consider ransomware sanctions risks within their SCP.

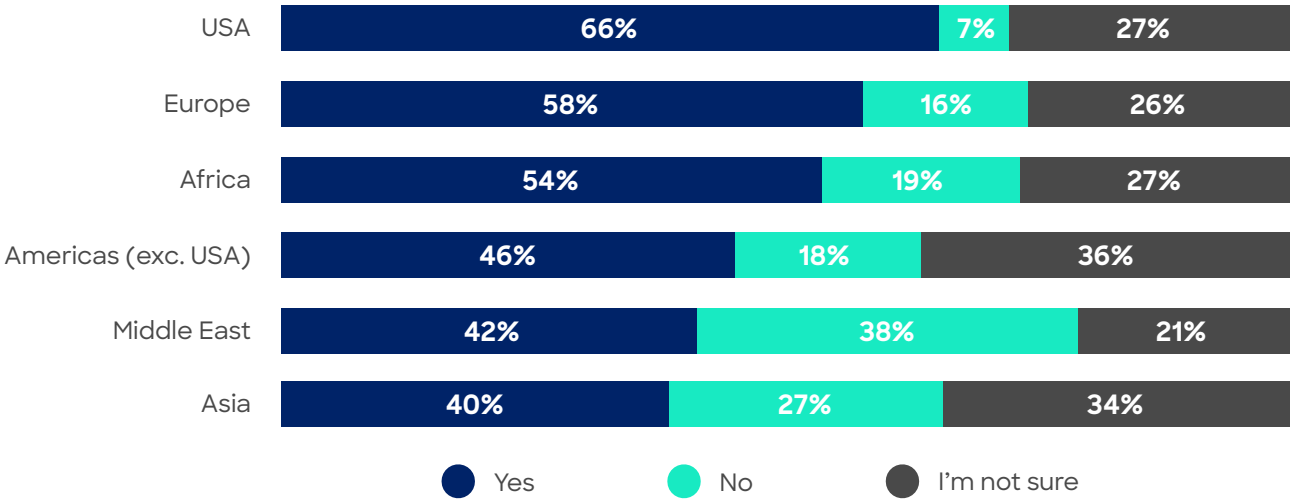
Are ransomware sanctions risks considered within the context of your organization's sanctions compliance program?



Base: all non-government respondents with a sanctions compliance program (311)

US respondents are most likely to have an incident response plan for ransomware attacks.

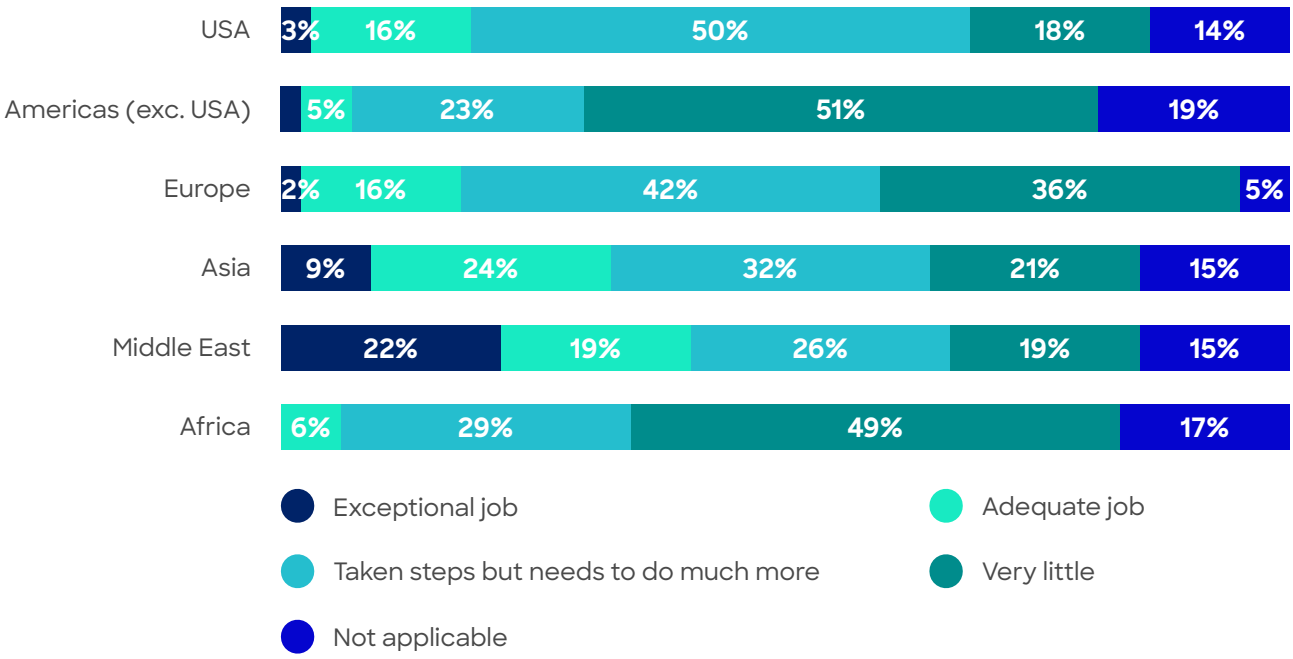
Do you have an organizational response plan/incident response plan for ransomware attacks?



Base: all non-government respondents (348)

Respondents in the Middle East are by far the most likely to view their government's efforts favourably.

How would you characterize your national government's efforts to provide information/ guidance to private sector organizations to safeguard against ransomware attacks?



Base: all respondents (395)

Key Takeaways and Recommendations

Key Takeaways from the Survey

- There is a distinct lack of familiarity with ransomware across the anti-financial crime community.
- Ransomware is viewed as a current and growing threat by the majority of respondents.
- There is widespread lack of familiarity with the potential sanctions risks that can result from ransomware and they are often not being factored into SCPs.
- Most respondents have taken steps to protect their organization from ransomware attacks in the past year, and there is a strong level of confidence in those measures.
- Anti-financial crime teams are often not involved in organizational ransomware response plans and investigations, particularly sanctions compliance teams, and there is a lack of specific policies and procedures on ransomware or specific training.
- It is generally perceived that national governments are not doing enough to shield private companies from ransomware, and additional information sharing, training, and emphasis on identifying and penalizing ransomware groups is needed.

Effectively Addressing the Threat: Recommendations

- This survey has demonstrated the need for the global compliance community to enhance their knowledge and understanding of the financial crime risks that can result from ransomware.
- Organizations should undertake an enterprise-wide risk management discussion. This discussion should include the facilitation of ransomware specific training, as well as the integration of sanctions and AFC – considering anti-financial crime obligations such as SAR filing – into their enterprise-wide incident response plan. Additionally, as part of sound risk management practices, organizations should develop a ransomware payment risk appetite statement and develop an aligned incident response plan.
- Both formal and informal information sharing mechanisms should be explored and executed to enable greater cohesion, reporting, and information sharing between the public and private sectors.
- Governments should consider development of a communication strategy that goes beyond issuance of guidance – providing training to industry and informing all sectors of threats, risk indicators, typologies, and how to work with law enforcement agencies.

ACAMS Next Steps

Over the coming months, ACAMS will be undertaking a concerted program of activity to support both industry and government to meet the threat of ransomware and build private sector organizational resilience. This will be primarily undertaken through cross-industry public-private dialogue, held via the Ransomware Workstream of the International Sanctions Compliance Task Force. Identified outputs include the development of a tabletop ransomware exercise simulating responding to a live ransomware attack, a position paper outlining best practices for mitigating ransomware sanctions risks, and training and masterclasses aimed at enhancing industry and government awareness of ransomware threats and vulnerabilities.