SURVEY REPORT

State of Ransomware for 2022 and Beyond

A look into insider threats, blame culture, and zero trust.

Introduction

Cybersecurity professionals around the world are currently facing adversity on all fronts. After operating through a global pandemic, the industry emerged in the midst of accelerated digital transformation initiatives supporting the move to the cloud. Since then, the exacerbation of the ransomware crisis means that security teams are now under enormous pressure to keep up with the increasing complexity of threats both externally and internally, overcome blind spots within their hybrid IT infrastructure and adhere to stringent cyber insurance requirements.

This concoction of challenges has meant that 59% of IT managers are expecting their organizations to experience a ransomware attack in the next 12 months. Yet only 4% are very confident that they are prepared for it, and 85% are worried they will face professional ramifications if the business were to be disrupted by ransomware.[1]

When things go wrong and ransomware is successfully deployed on a corporate network, many are quick to point the finger and blame CIOs and CISOs even if they never had the influence, investment or visibility to sufficiently improve their security infrastructure.

To mitigate these problems, security teams have looked to a variety of solutions. In 2020, Gigamon released a report on attitudes towards zero trust and whether it was viewed as a useful framework within a complex environment. We found that perceptions of this architecture in EMEA were evolving, and zero trust was viewed by 61% of respondents as a way to enhance their IT strategy.[2]

This latest survey report looks into whether these attitudes towards zero trust have changed, as well as how the increasingly complex hybrid IT environment and the rise in ransomware continues to affect security professionals across the world. It analyzes the feedback from across six key global markets – the US, UK, France, Germany, Australia and Singapore – to identify how the threatscape is changing and the severity of the 'blame culture' in cybersecurity. The report also addresses the critical role that 'deep observability' – i.e., the addition of real-time network-level intelligence to amplify the power of metric, event, log and trace-based monitoring and observability tools – has to play in supporting the cybersecurity industry as it attempts to tackle all of these issues.

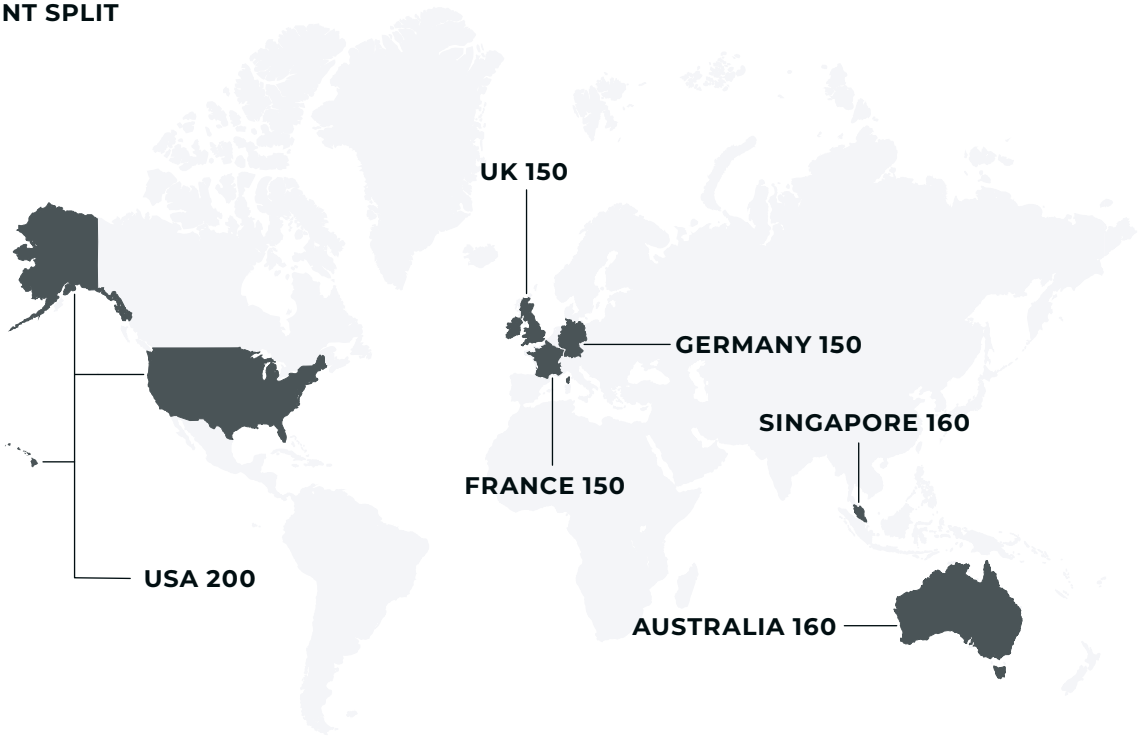
Methodology

The data used within this report was conducted by Vitreous World, which adopted an online methodology and recruited a mix of CIOs, CISOs, CTOs, COOs, Network Managers, Director of Network Operations, Network Architects and other security titles. Interviews were conducted in the UK, France, Germany, the USA, Australia and Singapore. All respondents were guaranteed to remain anonymous as part of the study.

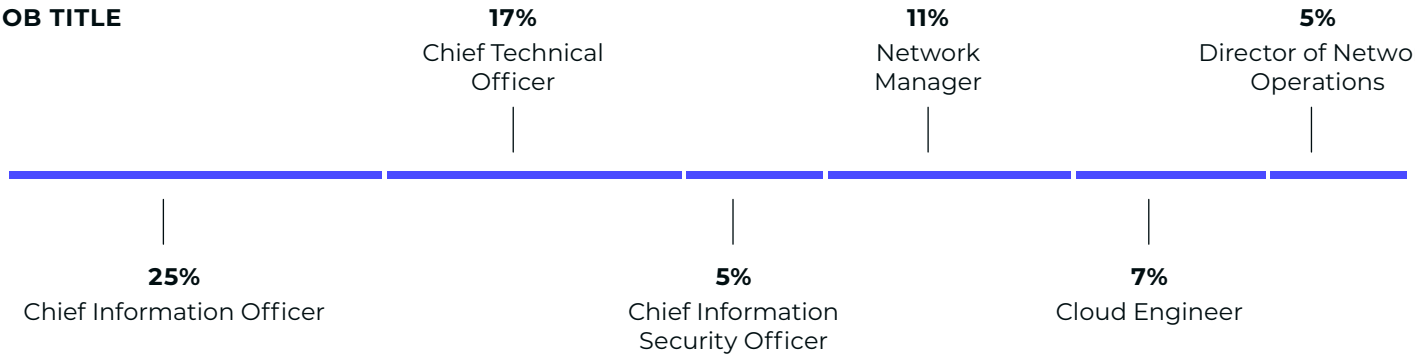
Fieldwork was carried out between 22nd of June and the 29th of June 2022. The sample comprised of the following professionals:

- **1,020** respondents split across the US (200), the UK (150), France (200), Germany (150), Australia (160) and Singapore (160)
- **43%** work for companies with between 501 and 1,000 employees, and **57%** work for companies with more than 1,000 employees
- **98%** work full time, **2%** part-time
- **Job titles included:**
  Chief Information Officer (25%),
  Chief Technology Officer (17%),
  Chief Information Security Officer (5%),
  Network Manager (11%),
  Cloud Engineer (7%) and
  Director of Network Operations (5%)

RESPONDENT SPLIT



JOB TITLE



The state of ransomware

A. INVESTMENT AND BOARD PRIORITIES

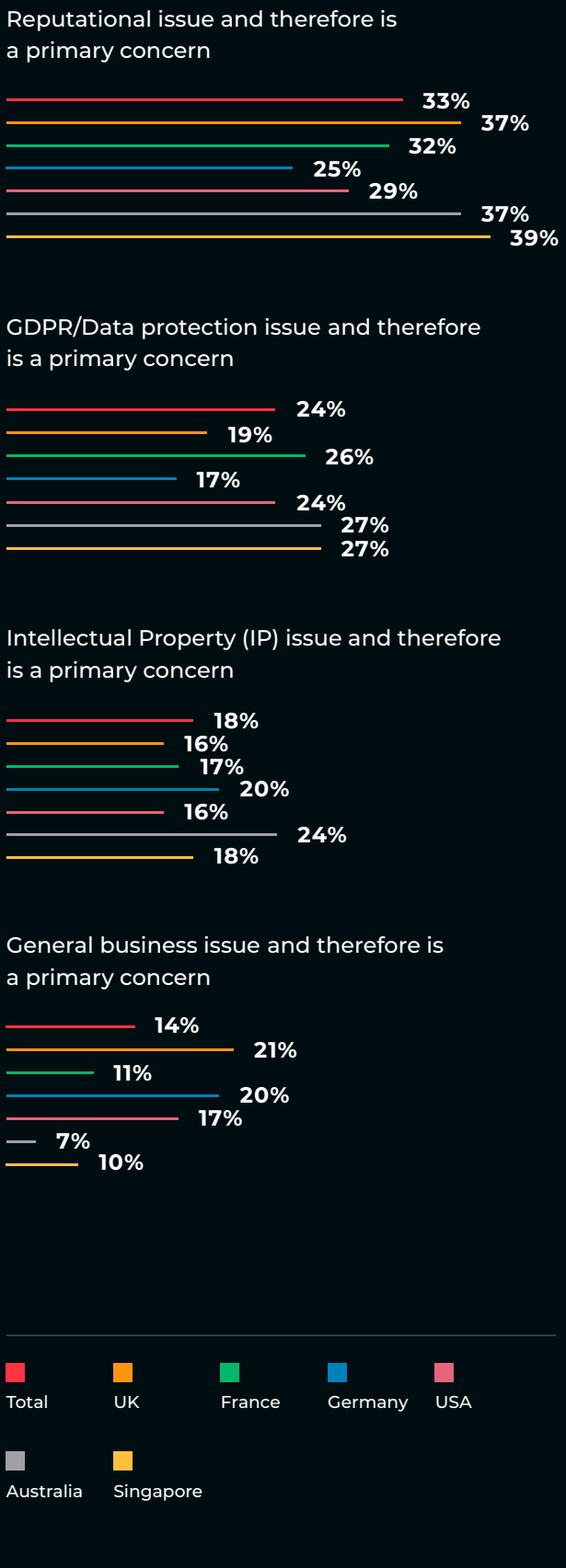
It is no secret that ransomware is wreaking havoc for security teams across the globe, but we wanted to identify whether it had truly penetrated boardroom discussions and influenced financial decisions in recent months.

Overall, **59%** of global respondents agreed that the ransomware crisis has worsened in the last three months and **95%** have experienced ransomware attacks in the last year. Yet at the same time, almost 1 in 2 **(45%)** believe infosecurity investment is going down. The results indicate that while the EMEA region believes that investment will continue into ransomware protection, the rest of the world is not as confident. In fact, nearly half **(49%)** of US respondents, and over half in Australia **(57%)** and Singapore **(58%)** believe it is decreasing.

The general consensus in EMEA is that investment will either continue or stay the same: **40%** of UK respondents disagreed when asked if they think investment is decreasing, along with **48%** in France and **37%** in Germany, compared to a much lower average of those that disagreed across APAC and the US **(26%)**.

How is ransomware viewed within your organization?

The board views ransomware as a/an:



Fortunately, ransomware remains on global boardroom agendas and it is viewed in various different ways. **89%** of global boardrooms see this threat as a priority concern, a number that rises in the UK **(93%)**, Australia **(94%)** and Singapore **(94%)**. Interestingly, when asked how this cyber threat is viewed, the leading perception across all regions was that it is a 'reputational issue' **(33%)**. In comparison, fewer respondents acknowledged that some boards believe ransomware is:

- A GDPR/Data Protection issue **(24%)**
- An intellectual property issue **(18%)**
- A general business issue **(14%)**

Only **1%** stated that ransomware isn't considered at all and never mentioned at board level.

B. CAUSES AND SOLUTIONS

When asked about the routes of any ransomware attacks respondents have seen in the last year, phishing **(58%)** and computer viruses – e.g., malware – **(56%)** dominated responses. In the UK in particular, phishing led even more significantly, with **71%** claiming they had seen it as a route source in recent months.

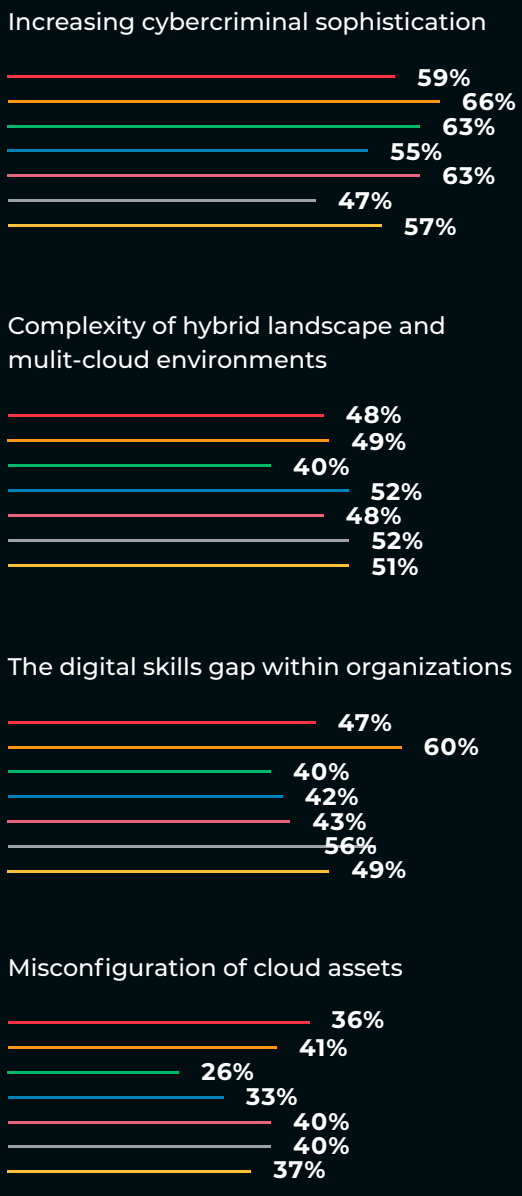
Cloud applications were also cited as a common ransomware attack vector, particularly by the UK **(53%)**, Australia **(51%)** and the US **(47%)**. In fact, US respondents placed third-party compromise on par with cloud applications – the only country to reference third-parties as such a common route for ransomware. However, considering some of the high-profile supply chain attacks across this region in recent years, this may come as little surprise.

We also wanted to know what security professionals are seeing as the biggest drivers and the central causes of ransomware exploits becoming more prevalent. What we found was that the increasing sophistication of cybercriminals is viewed worldwide **(59%)** as one of, if not the leading cause behind this worsening crisis. This number rose to **66%** in the UK and **63%** in both the US and France. It is compacted by:

- The growing complexity within the hybrid and multi-cloud environments **(48%)**
- The digital skills gap **(47%)**, seen most critical by UK respondents **(60%)**
- Misconfiguration of cloud assets **(36%)**, particularly problematic in the US **(40%)**, Australia **(40%)** and the UK **(41%)**

The fact that cloud misconfiguration is being seen as a driver for ransomware may signify a failure of the 'shared responsibility model', as those moving to a virtual or hybrid environment may not fully comprehend their role in security.

What do you believe are the central causes for ransomware exploits becoming more prevalent?



To combat these issues, **87%** of global respondents agree – or strongly agree – that they need greater visibility to identify where ransomware may be hiding in their hybrid and multi-cloud environments. It's clear that with the compound challenges of less resource, greater cloud to core complexity and cloud misconfiguration, visibility is integral to mitigating ransomware risk. Without a more holistic view, it becomes impossible to manage or protect against the most sophisticated attacks. This is particularly pertinent given that average adversary dwell times are now over 285 days.[3]

87% of global respondents agree – or strongly agree – that they need greater visibility to identify where ransomware may be hiding in their hybrid and multi-cloud environments.

The survey also found that security professionals recognize the benefits of a wide range of solutions for mitigating ransomware attacks. **80%** of global respondents agree that mandatory reporting, as enforced by government bodies, would improve their organization's security posture. What's more, the top focus points for dealing with ransomware are:

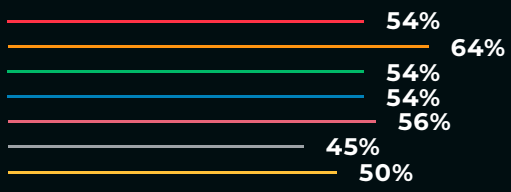
- Investment in more cybersecurity tooling **(56%)**
- Security awareness and training **(54%)**
- Adopting a zero trust Architecture **(47%)**
- Enabling deep observability – holistic visibility – across the entire IT infrastructure **(45%)**

It's clear that with the compound challenges of less resource, greater cloud to core complexity and cloud misconfiguration, visibility is integral to mitigating ransomware risk.

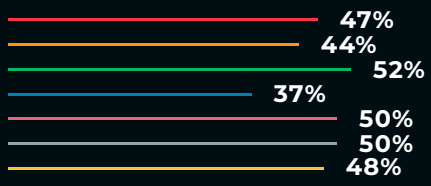
Which areas are being considered as a focus point for dealing with ransomware attacks?

Investment in more cybersecurity tooling

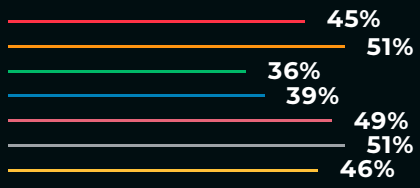
Security awareness and training for all employees



Adopting a zero trust architecture



Enabling deep observability (holistic visibility) across the entire IT infastructure



Total UK France Germany USA

Australia Singapore

The number of solutions rated globally, with such small margins in between, suggests that professionals view a layered approach to security as best; it's not just one area that needs to be considered in order to bolster defences against ransomware. With 'Defence-in-Depth' as a core architectural security principle, it is positive that a multi-faceted approach is recognized and should be a focus for all enterprises. Solutions like implementing a cybersecurity committee **(39%)**, taking out cyber insurance **(30%)** and outsourcing security requirements **(24%)** were less popular.

60% of global respondents agree the security tools that they're currently using are not as effective without complete visibility.

Yet while investment in more tooling may be the top solution identified, organizations can't continue to keep throwing more tooling at security issues. The survey also found that **60%** of global respondents agree the security tools that they're currently using are not as effective without complete visibility. Therefore, optimization through visibility is recognized as invaluable.

C. DEEP OBSERVABILITY

Deep observability defined

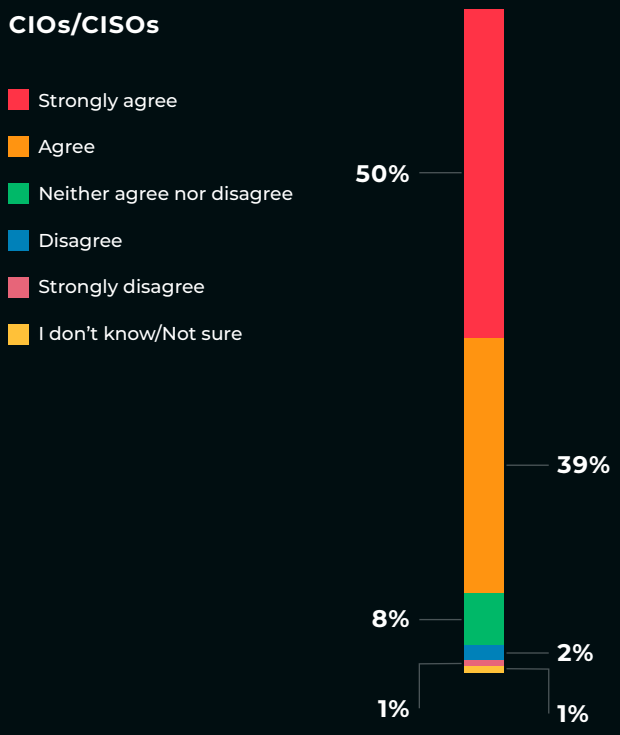
The addition of real-time network-level intelligence to amplify the power of metric, event, log and trace-based monitoring and observability tools to mitigate security risk, deliver a superior user experience, and ease operational complexity.

Named within one of the top focus points for dealing with ransomware attacks, 'deep observability' is becoming increasingly synonymous with ransomware protection, particularly within the cloud. We learned that **89%** of global security leaders surveyed agree deep observability is an important element of cloud security – and **50%** of global CISOs/CIOs strongly agree with this statement. What's more, **82%** believe that deep observability is part of a safe migration to the cloud.

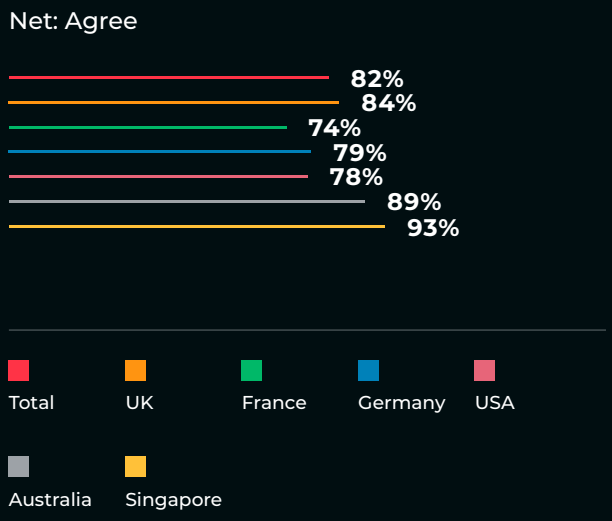
Just like ransomware, it is also being recognized as a priority by the board. **78%** of global respondents agree that deep observability is being discussed in the boardroom for better network to cloud security – a number that rises to **86%** in Australia and **85%** for global CISOs/CIOs.

It seems the benefits of visibility are clearly understood globally: **80%** agree that having access to raw packet data can unlock deep insight and strengthen a security posture. However, some regions are not yet recognizing this as 'deep observability'. Namely, only **36%** and **39%** in France and Germany respectively noted it was an area being considered in ransomware protection. This signifies that while this relatively new category is making waves across countries like the UK and US, there is still education to be done on its value in other regions.

Deep observability is an important element of cloud security. To what extent do you agree or disagree?



Deep observability is part of safe migration to the cloud. To what extent do you agree or disagree?



Cyber insurance may be exacerbating the ransomware crisis

Cyber insurance is listed as another solution that security professionals are turning to in the wake of the ransomware crisis, although not as commonly as more proactive measures. This may be due to rising premiums prices and the tightening of policies. For instance, price of cover increased by **130%** in the US, and **92%** in the UK, in the fourth quarter of 2021 alone.4 However, certain regions appear more confident in its value than others, even if many also link it to the rise in ransomware itself.

We found that Australia **(94%)** and Singapore **(93%)** have the highest number of organizations with cyber insurance, although it is seen as valuable consistently around the world, and as a key component within enterprise security strategies. The UK has the lowest adoption, with over **20%** of organizations without cyber insurance at all, followed by France **(15%)**, Germany **(15%)** and the US **(14%)**.

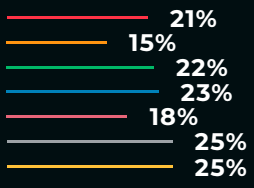
The worrying finding however, is that over one fifth **(21%)** of organizations surveyed – and one quarter within APAC – claimed that cyber insurance is their entire cybersecurity strategy: they do not have other processes or tools in place.

At the same time, **57%** of those surveyed also agreed that the cyber insurance market is exacerbating the ransomware crisis. In APAC, where cyber insurance is most commonly used, this concern is felt by **66%** of Australian respondents and 68% of those in Singapore. Therefore, while this area of the world is heavily relying on the cyber insurance solution, enterprises here simultaneously worry about its longevity and longterm effect on the cyber environment.

It appears this concern permeates on a global scale, as at least half of all respondents agree that cyber insurance is exacerbating the ransomware crisis, including **60%** in the UK. Therefore, a shift needs to take place to ensure the insurance industry is supporting enterprises rather than catalyzing future attacks. For better cyber hygiene, it is also crucial that those organizations without proactive measures in place, and that rely solely on cyber insurance as their protection, change their approach.

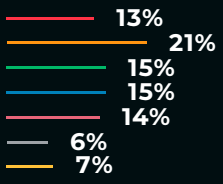
Which of the following options best reflects your organization's current position on cyber insurance?

Having cyber insurance is our cybersecurity strategy. We don't have other processes or tools in place.

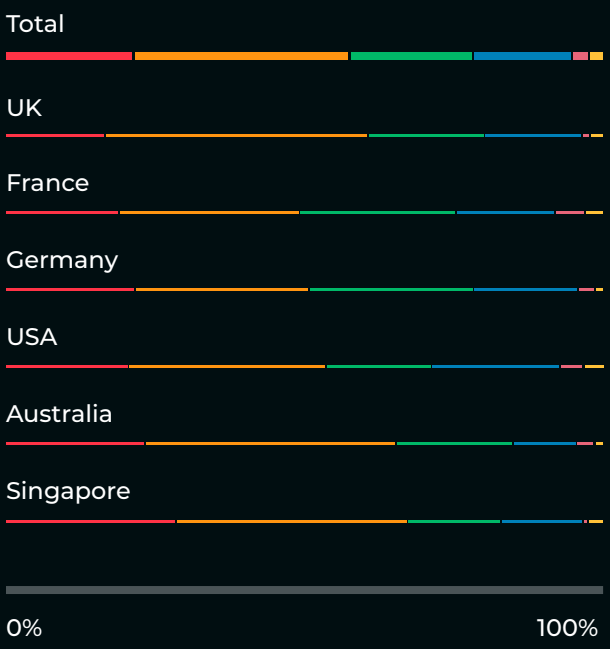


Cyber insurance makes up a component of our cybersecurity strategy. We have a range of other tools and processes in place.

We do not currently have cyber insurance.



The cyber insurance market is exacerbating the ransomware crisis. To what extent do you agree or disagree?



- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree
- I don't know/Not sure

The malicious insider threat is not an uncommon route for ransomware

With phishing emails considered the top source of ransomware attacks in the last 12 months, security professionals undoubtedly need to be concerned about the risk of the insider threat and the consequences of internal teams accidentally clicking a dangerous link.

The malicious insider – a security risk that originates from within the targeted organization – is far less discussed. Yet, we wanted to identify whether this is a legitimate risk, if security professionals have strategies in place to mitigate such a risk and what it means for ransomware.

We found that of those who believe general insider threats are a central cause for an increase in ransomware attacks, **95%** (and **99%** of CISOs/CIOs) view the malicious insider as a significant risk. What's more, this type of insider threat is seen as a route for ransomware attacks by almost one in three organizations worldwide **(29%)**.

The good news is that **66%** of those who are seeing this as a cause of ransomware now have a strategy for both types of insider threat – accidental and malicious – particularly in the case of Singapore **(80%)**, Australia **(73%)** and the US **(67%)**. Of the CISOs/CIOs that view malicious insiders as a threat, **91%** look to staff awareness and training to mitigate the risk, alongside Zero trust **(66%)** and deep observability **(66%)**. For security professionals the UK and US, **81%** and **75%** respectively cited this holistic visibility across entire IT infrastructures through deep observability as a mitigation strategy.

However, it seems greater observability is needed. According to respondents, many do not have visibility to distinguish which type of insider threat is endangering their business. This issue is most prominent for the UK and German markets, with **40%** and **41%** agreeing respectively.

Therefore, despite rarely headlining discussions, the malicious insider threat is viewed as high risk by many security professionals around the world. In fact, only **6%** more of global respondents are seeing accidental insiders as a more common route than malicious insiders for ransomware – despite far more attention being dedicated to mitigating the accidental risk. To help counter this threat, however, a deeper level of visibility is needed.

Do you believe the malicious insider threat is a significant threat to your business?

Yes. We have a strategy in place that deals with both accidental and malicious insider threats.

66%
56%
64%
51%
67%
73%
80%

Maybe. We know it is a threat, but we don't have the visibility to distinguish between the two types of insider threats.

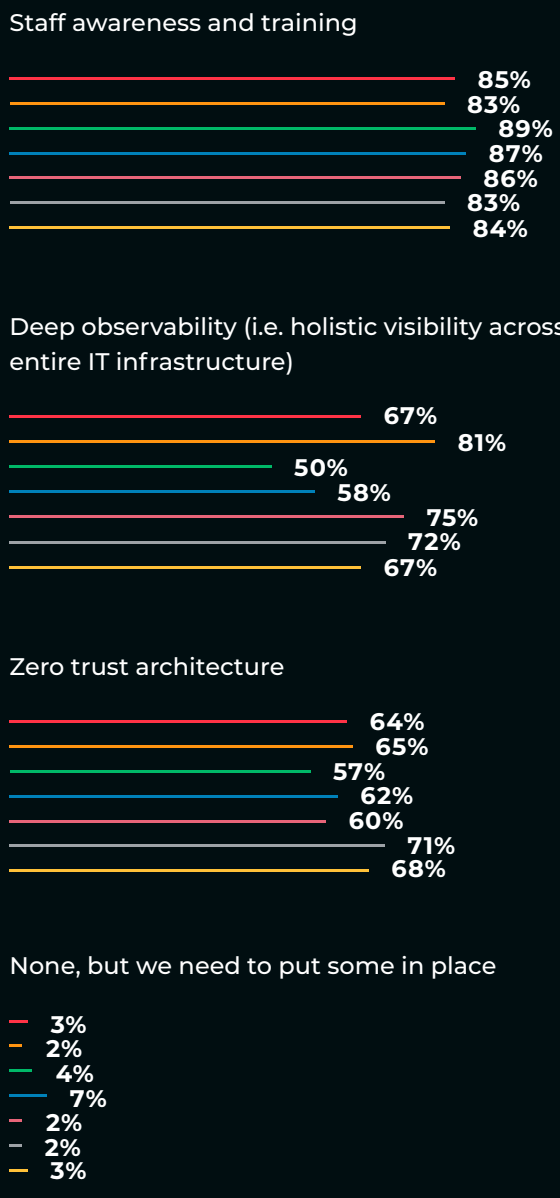
29%
40%
29%
41%
25%
25%
20%

No. We do not see the malicious employee stealing sensitive data as a threat.

5%
4%
7%
8%
9%
2%
0%

Total
UK
France
Germany
USA
Australia
Singapore

What measures, if any, does your organization have in place in order to mitigate the risk if insider threats are to turn malicious and support ransomware operators?



The global consensus of a cybersecurity blame culture

The growing ransomware crisis, rising cyber insurance premiums and risk of internal threats becoming malicious, all contribute to a more dangerous threat landscape. As more organizations fall victim to this landscape, fingers inevitably point to the CIOs and CISOs responsible for protecting their infrastructure and a 'blame culture' is automatically established.

By blame culture, we mean:

an environment within which there is a tendency to look for one person/a group of people/a team that can be singled out, held responsible, and criticized for an error, negative occurrence or mistake, irrespective of their actual culpability.

We decided to interrogate this concept and analyze to what extent this culture exists, the effect it may be having on ransomware preparedness and whether there is light at the end of the tunnel.

The results vary from region to region, but overall, **88%** of global respondents believe a blame culture exists at least somewhat in the industry – a number that rises to **90%** for CISOs/CIOs, **95%** in Australia and **92%** in the US. In fact, in the US **38%** see it as 'heavily prevalent', along with **37%** in Singapore, implying that while blame culture exists on a global scale, it is the US and Singaporean markets that feel it most intensely.

1 IN 3 CIOs/CISOs believe the blame culture is heavily prevalent in cybersecurity.

Professionals in the UK have also expressed concern around the issue of blame culture, and **32%** believe that finger pointing leading to a lack of transparency as to the state of IT infrastructure is a central cause for ransomware exploits becoming more prevalent.

The results are similar for Australia: **30%** see finger pointing as a direct cause of worsening ransomware exploits, while a third **(33%)** believe workforce burnout and CISO/CIO fatigue is causing the same issues. It seems therefore, that Australia's cybersecurity market is at a critical point, where a cultural shift is needed to support its professionals.

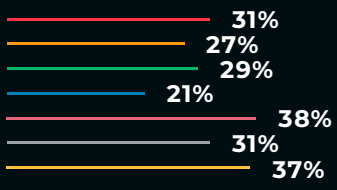
The result of this blame culture around the world is further difficulty for cybersecurity teams. Worryingly, **94%** of respondents who believe there is a blame culture in the industry told us that this could be a deterrent to the speed of reporting an incident – at least somewhat, depending on the scale of the incident. APAC is more confident in its belief that reporting is being delayed by a finger pointing culture – with **54%** in Singapore, **51%** in Australia agreeing. However, the US is not far behind at **45%**, along with **51%** of global CISOs/CIOs.

In other words, only **6%** feel that there is absolutely no delay in reporting of ransomware due to the blame culture. Such a small number indicates that this issue is endemic across industries, where security professionals are so reluctant to be the object of blame, they delay reporting and remediation. Undoubtedly, something needs to change.

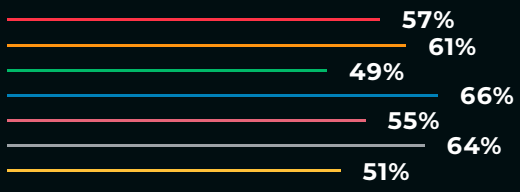
94% of respondents who believe there is a blame culture in the industry told us that this could be a deterrent to the speed of reporting an incident.

Do you believe a 'blame culture' exists in cybersecurity?

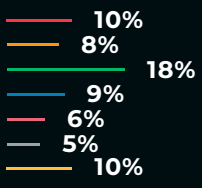
Yes. The blame culture is heavily prevalent; it is too easy to point the finger at the security team.



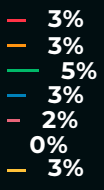
Somewhat. The blame culture does exist somewhat, mainly following a security breach or security/human error.

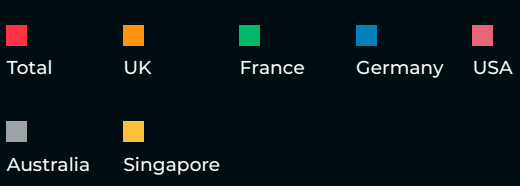


No. There is no blame culture at all within cybersecurity.



Not sure. I don't have an opinion on this.





However, there is good news: the blame culture is a fixable evil. Only **1%** of those surveyed claimed otherwise. The following solutions were indicated to be the most useful when eradicating the issue:

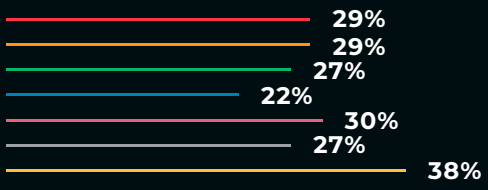
- Have a more open and transparent culture within an organization **(42%)**
- Focus on industry-wide collaboration and a security-first mindset **(29%)**
- Provide CIO/CISOs with full visibility (deep observability) into their infrastructure **(22%)**

In fact, over a quarter **(26%)** of CISOs/CIOs claimed they want more visibility through deep observability, so that they have the right level of insight to detect and respond to threats and can therefore overcome the culture of blame affecting the global cybersecurity community. Australia **(31%)** and the US **(24%)** also view this as a valuable solution.

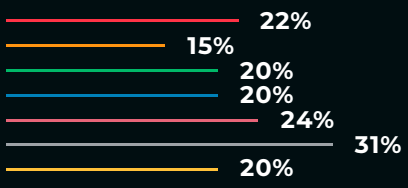
What do you think is the most effective way to eradicate the blame culture within cybersecurity?

Have a more open and transparent culture within an organization where security is deemed a collective responsibility.

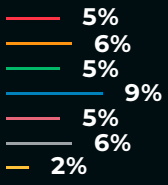
Focus on industry wide collaboration and instill a security first mindset across the company, which starts with educating staff.



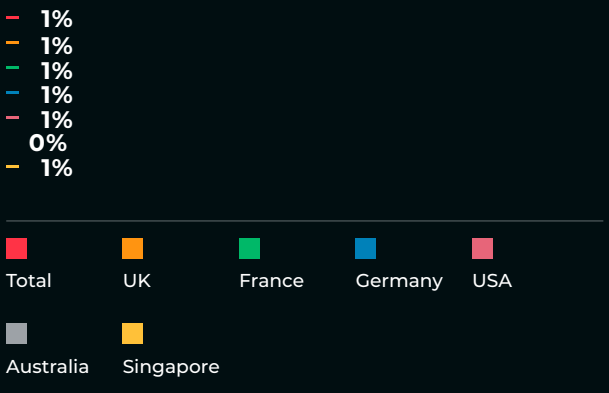
Provide CIOs/CISOs with full visibility (i.e., deep observability) into their infrastructure so that when a breach does occur, they have the right level of insight to detect threats and respond to them to mitigate risk.



Documentation of the risk, as well as records of any denial of budget that may lead to a breach.



I don't think there is an effective way to eradicate the blame culture within cyber security.



Zero trust

A. INVESTMENT AND BOARD PRIORITIES

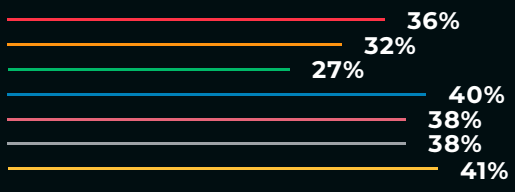
Across this ‘State of Ransomware’ report, zero trust is cited as a key element of an enterprise cybersecurity strategy, seen as important to mitigate both ransomware and malicious insider threats.

However, we also wanted to uncover exactly how attitudes towards this framework have changed in the two years since the last Gigamon survey and whether teams are any closer to embracing this security architecture.

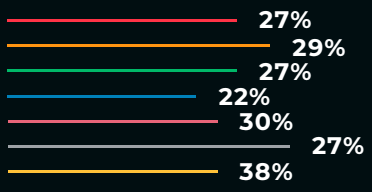
What we found was that boardrooms are now more invested in zero trust. Two years ago, for instance, only **53%** of UK respondents agreed that the framework was talked about openly at board level, compared to **67%** today. Across the rest of the world, over half **(58%)** of all security professionals agree that zero trust is discussed by the board.

What is the central benefit that you would use/have used to justify investment into a zero trust architecture to the board?

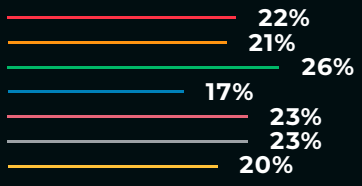
Risk management. With zero trust comes more control to manage (and therefore reduce) risk of data breaches.



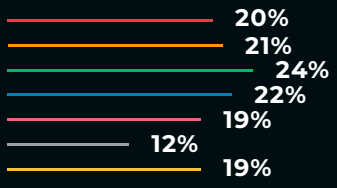
Brand and reputation. Better cyber hygiene protects the organization's reputation from high-profile breaches.



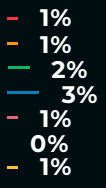
Customer protection. Organizations need stringent security frameworks primarily to protect their customer's data.

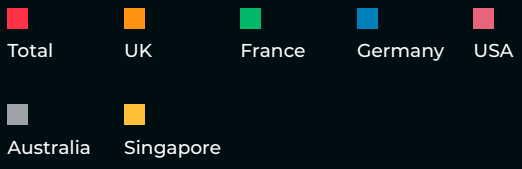


Productivity. Less network downtime and security breaches will improve the SecOps teams' productivity levels.



None of the above. It does not need justification from the Board





Importantly, of those that disagreed, over three quarters **(76%)** stated that it at least forms part of their digital strategy and is therefore handled by the CIO. Therefore, less than **15%** of those surveyed do not see zero trust as either a boardroom discussion or an element of their digital strategy.

We also asked how investment in zero trust is justified to the board. **36%** of respondents stated they portrayed the central benefit to financial decision-makers as 'risk management', while only **20%** used productivity as their justifier. However, in our last survey, we learned that **87%** of respondents had identified productivity – with less network downtime and security issues to remediate – as one of the biggest drivers for zero trust implementation. Therefore, security professionals may want to consider this argument in future discussions with the board.

B. AWARENESS AND UNDERSTANDING

Security professionals today are also beginning to understand the reality of what 'zero trust' means and how it can be implemented.

Around three quarters of global respondents agreed in this survey, as well as in the last report, that zero trust is a journey and not a tick-box exercise. However, awareness is growing of how challenging this infrastructure is as a security solution. Two years ago, **77%** of EMEA respondents saw zero trust as attainable, but now only **53%** agree. What's more, almost half **(48%)** of Australian respondents believe it is unattainable and **68%** are pursuing alternatives, while **20%** of those in France now disagree that zero trust is wise to consider.

What this means is that zero trust is no longer a buzzword, but a recognized framework that is not a quick solution. Instead, it is an extensive and challenging approach to better cybersecurity. This finding is backedup with learnings that **44%** of EMEA now believe that zero trust requires too much oversight and resource. Two years ago, this number was only **23%**.

Zero trust is no longer a buzzword, but a recognized framework that is not a quick solution. Instead, it is an extensive and challenging approach to better cybersecurity.

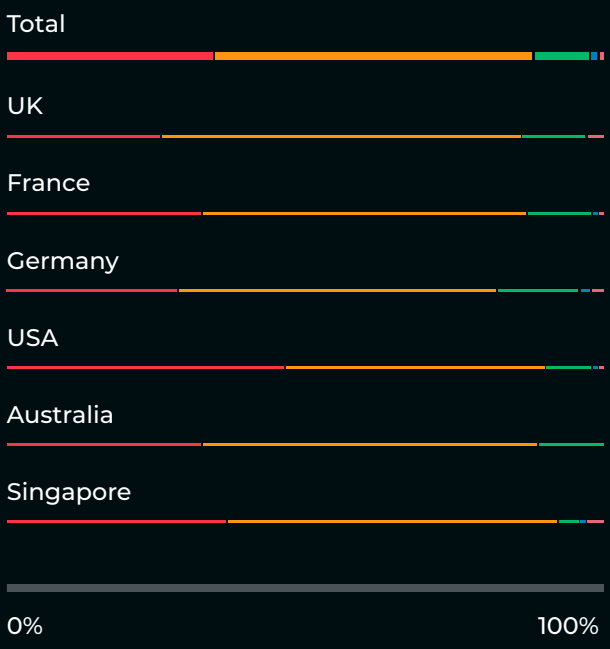
However, security professionals around the world are not ruling out zero trust completely, if at all. **63%** in the UK and **59%** in the US agree that this framework is attainable, and global respondents see it as a big trend in IT in the next 18 months (**80%** of CISOs/CIOs, for example).

What's more, while two years ago only **51%** of EMEA claimed to be comfortable implementing zero trust in the next three years, that number has now risen significantly to **83%**. This tells us that although zero trust may be unattainable for some right now, it is certainly a priority on the horizon. Of all the countries, it is the US that demonstrates the highest score for 'very comfortable' at **37%**, closely followed by Singapore **(34%)** and Australia **(33%)**.

To make this implementation possible, **98%** of global respondents agree that deep observability is at least loosely connected to zero trust – and **89%** say it is somewhat to strongly connected. In the US, there is the most confidence on this overlap, with **47%** claiming the two are strongly connected. It therefore seems the US market is leading the charge to zero trust, with a good understanding of how and why visibility is so important to cybersecurity.

In fact, with visibility into all areas of an IT infrastructure critical to allowing permissions across accounts and devices, it seems many are recognizing that while zero trust may be difficult, deep observability is certainly a pre-requisite and will make the journey far easier.

How strongly connected is deep observability to the successful implementation of a zero trust framework?



Key learnings

Ransomware is a board priority, especially given the increased sophistication of cybercriminals

As the ransomware crisis continues, and cybercriminals evolve their Tactics, Techniques and Procedures (TTPs), the boardroom is making this threat a priority within their discussions. Many are most worried about ransomware affecting their organization's reputation.

The malicious insider threat is a significant risk and route for ransomware

While accidental insider threat is often seen as the more common of the two, the risk of the malicious insider appears to be on the rise. Not only is the purposeful breach of data seen as a threat by almost all security professionals, it has been noted as a route for ransomware in recent months. Fortunately, strategies to mitigate this are in place in most enterprises.

There's a blame culture slowing down incident reporting, particularly affecting the US and Singapore

The US and Singapore have demonstrated the most concern around a 'blame culture' of finger pointing within the cybersecurity industry. Around the world this issue is causing delays in incident reporting, yet it is seen as possible to overcome with more transparency, collaboration and visibility.

Awareness of zero trust has grown, with many now aware of its complexities

Perceptions of zero trust have changed significantly in EMEA in the last two years. As security professionals have learned exactly what this architecture entails, they have less confidence in its attainability right now. However, around the world many feel comfortable implementing zero trust in the next three years, and they see risk management as the primary justification for doing so.

Deep observability is considered key to cloud security and zero trust

The concept of 'deep observability' is valued by most and viewed as an integral part to both migration to the cloud environment and security within the cloud. In terms of zero trust, it is the US that is most confident in the role that deep observability plays in making this architecture a possibility.

Find out how to tackle the ransomware crisis with deep observability from cloud to core.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide.

To learn more, please visit gigamon.com.

Resources

[1] Gigamon and Gartner Peer Insights, Network Visibility and Ransomware. https://www.gigamon.com/content/dam/resource-library/english/analyst-industry-report/ar-gartner-peer-insights-network-visibility-and-ransomware.pdf

[2] Gigamon, Zero trust Survey. https://www.gigamon.com/campaigns/zero-trust-survey.html

[3] IBM, Cost of a Data Breach Report 2021. https://www.ibm.com/security/data-breach

[4] Marsh, Global Insurance Market Index. https://www.marsh.com/uk/services/international-placement-services/insights/global_insurance_market_index.html

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com