AI & Partners

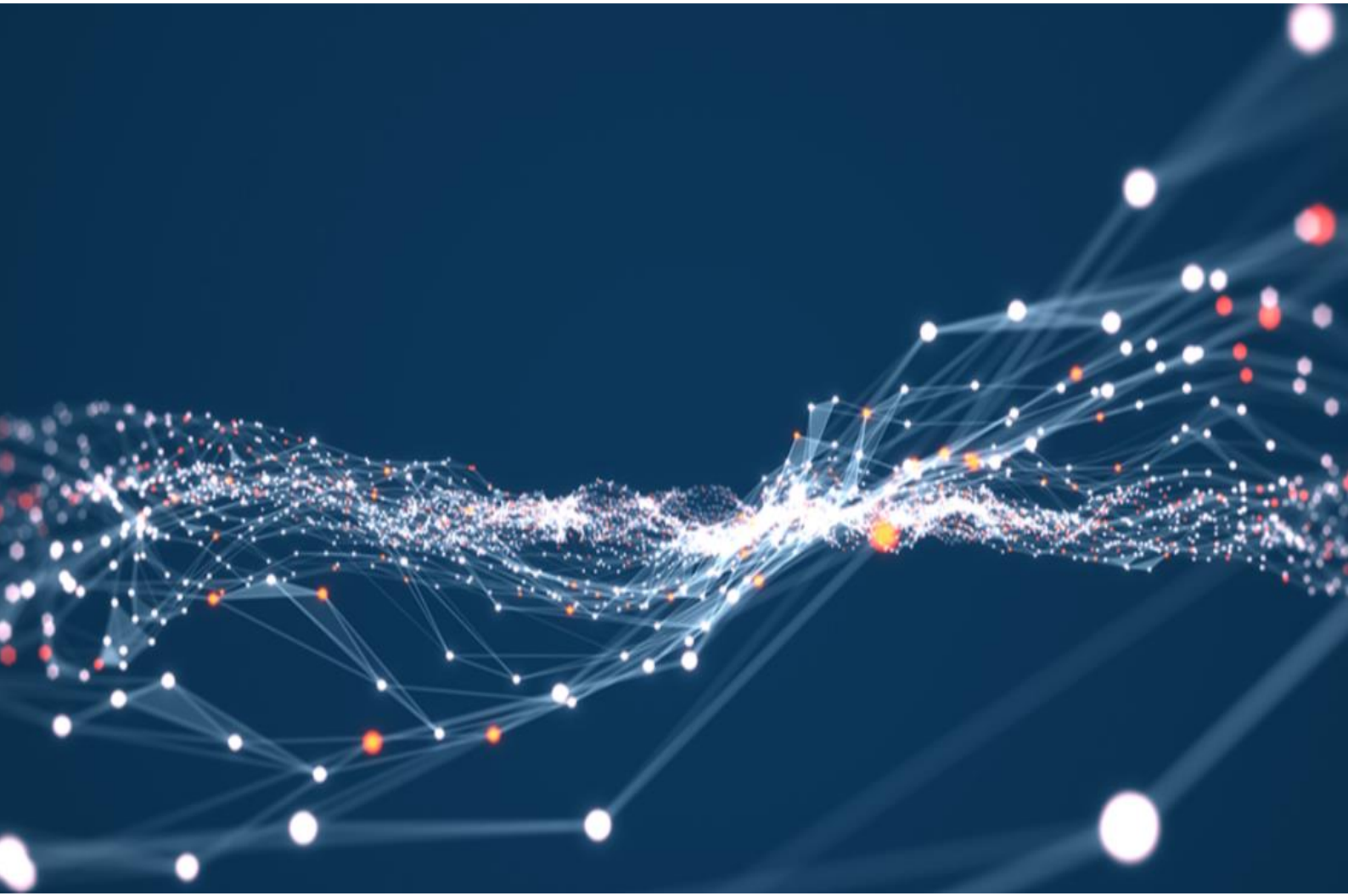
Amsterdam - London - Singapore

EU AI Act

Cyber Security Outcomes

Examining the potential impact of the forthcoming EU Artificial Intelligence (AI) Act on cyber security outcomes across all industries following its entry into force on 1st August 2024

August 2024



AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Our report finds that the EU AI Act is likely to motivate organisations to make improvements to their cyber risk management, even though it is clear that many of these improvements are being maintained. Moreover, our data suggests that most organisations are potentially introducing new or improved AI governance and other cyber security policies, processes, and procedures and technical controls, including measures to protect AI systems and that data that supports them against a cyber-attack, with less change being evident in relation to procurement and supply chain risk management.

About this report

This report is based on market research, publicly available data, and interviews with AI specialists in AI & Partners, financial services organisations, and relevant third-parties. Moreover, quotations provided on specific topics reflect those of AI specialists at AI & Partners to be as representative as possible of real-world conditions. All references to EU AI Act reflect the version of text valid as at 13 June 2024. Accessible here.

Contents

Part.1 Executive Summary

Context

Growing sentiment intimates that cyber risk management can be achieved through the implementation of the European Union ("EU") artificial intelligence ("AI") Act (the "EU AI Act" or "Act"). This position is informed by extrapolating the findings of study conducted by RSM on the impact of the General Data Protection Regulation ("GDPR") on cyber security outcomes, which included a review of existing literature and both quantitative and qualitative fieldwork and analysis (the "Study")[1]. Findings from the Study will inform new reviews of cyber security incentives and regulations which are forthcoming and tie into related provisions under the EU AI Act, such as those contained in Article 15..

This paper was written particularly in light of the recent global information technology ("IT") outage on Friday 29th July 2024 caused an update to anti-virus software belonging to CrowdStrike, a cyber-security firm, designed to protect Microsoft Windows devices from malicious attacks[2]. While the attack was by not caused by a cyber incident, it provides a concrete example to analyse the broader implications of the EU AI Act on cybersecurity. Moreover, it highlights the need for stringent regulatory measures, risk management, transparency, and accountability in AI systems to prevent such incidents. The whitepaper can serve as a comprehensive guide for stakeholders to navigate the intersection of AI regulation and cybersecurity, ensuring safer and more reliable outcomes.

Key findings

Existing literature on the potential impact of the EU AI Act is scarce, especially the impact of the EU AI Act on individual countries. Thus, firm conclusions on their impact on individual countries, included the United Kingdom ("UK"), specifically cannot be drawn from existing research. Notwithstanding, using results from primary research contained in the Study, it is clear that most organisations are likely to improved their cyber security when measured against relevant standards.

Moreover, the Study indicates that most organisations are likely to have increased their prioritisation of cyber security, including Board level prioritisation, as well as increasing their spend in this area. Most organisations are estimated to have also introduced new or improved cyber security policies, processes, procedures and technical controls, which can be expanded to include measures to protect AI systems and the systems that protect these against cyber-attacks.

It is encouraging to put forward the following estimations (likely % respondents in brackets):

- most organisations have some form of cyber security strategy (69%)
- most Board members receive updates on cyber security at least once a quarter (52%)
- where organisations had employees that specialised in cyber security, the majority create one or more of these roles over the next 3 years (77% and 81%, respectively)

While organisations are likely to identify a range of factors that influence these changes in their cyber security over the next 3 years, those potentially linked to the EU AI Act are considered the most important (23% likely to say that the introduction of the EU AI Act is the most important factor). The vast majority of organisations (82%) are also likely to say that all of the changes in their cyber security will be as a result of the entry into force of the EU AI Act at least to a small extent.

[1] RSM, (2020), 'Impact of the GDPR on Cyber Security Outcomes | Final Report (August 2020)', accessible at https://assets.publishing.service.gov.uk/media/5f294433d3bf7f1b18aaad27/Impact_of_GDPR_on_cyber_security_outcomes.pdf (last accessed 20th July 2024)
[2] BBC, (2024), 'CrowdStrike and Microsoft: What we know about global IT outage', accessible at https://www.bbc.com/news/articles/cp4wnrxqlewo (last accessed 19th July 2024)

Data can also be broken down into groups of specific interest, chosen to understand in greater detail how the potential impact of the EU AI Act may vary across different contexts. This includes those who are likely to experience a cyber security incident, completed a Fundamental Rights Impact Assessment4 ("FRIA") or deployed AI systems, as well as large businesses, large businesses with complex and interconnected supply chains, Managed Service Providers ("MSPs"), Local Authorities ("LAs") and non-profits providing important public services, Small or Medium-sized Enterprises ("SMEs") and across different industries. The research indicates that that the potential impact of the EU AI Act will vary according to certain organisational characteristics.

Organisations that conduct a FRIA, those that deploy AI systems, and those that experience a cyber security incident are potentially more likely to improve their cyber security measures in the next 3 years. It is important to note, however, that there is some overlap between these 3 groups. This suggests that the EU AI Act can successfully encourage improvements in cyber risk management for organisations that are within the scope of the regulation. Experiencing an incident also appears to potentially encourage organisations to act, suggesting that when organisations have knowledge of the damage a breach can have, they are going to be more likely to make improvements. Giving organisations this insight in advance of an incident may help incentivise them to act in future, without having to experience an incident directly.

As shown by the Study, it also indicate that improvements are potentially not going to be realised equally across all aspects of cyber security. Although the primary research indicates that most organisations are likely to improve their cyber risk management in the next 3 years, more improvements are likely to be reported in relation to governance, risk management, data security and systems security, while less change will be evident in relation to procurement and supply chain risk management. Organisations are also perceived to be more likely to have made changes to AI than other aspects of cyber security. This potentially suggests that organisations could benefit from taking a resilience approach, emphasising the importance of improving the detect, respond and recover aspects of cyber security, as well as preventative aspects.

The likely changes to be made as a result of the EU AI Act's entry into force are estimated to be sustained in the vast majority of organisations (84%). Challenges to sustainability related to the ongoing costs associated with maintaining compliance and staff awareness of the EU AI Act are anticipated to be an ongoing issue. It may be too soon to determine whether these changes can result in a longer-term behaviour change or a cultural shift towards more robust practices. This is a potential area for further research in the future.

Where organisations are not likely to change their cyber security practices in the next 3 years, in the majority of cases, it is perceived to be because they felt their existing measures were sufficient (61%). Organisations are likely to be confident in their ability to manage risks, protect against attacks, detect threats and minimise the impact of an incident because they had robust policies and procedures in place, and their staff had appropriate cyber security expertise. It is possible, however, that for some organisations this projected confidence may be misplaced. They may still benefit from assistance in assessing their risk posture and the appropriateness of the measures they have taken.

Some organisations are likely to report detrimental impacts as a result of the EU AI Act:

- 50% perceived to say that the EU AI Act leads to excessive caution amongst staff in the handling of AI systems
- 36% perceived to report excessive focus on AI governance to the detriment of other aspects of cyber security

- 27% envisaged to report excessive investment in cyber security, significantly beyond what is necessary
- 78% anticipated to say that cyber security updates will become more focused on aspects of AI governance than general cyber security

This suggests that organisations could benefit from guidance on the appropriate balance between elements of AI governance and other aspects of cyber security.

The evidence also implied that the EU AI Act will potentially not impact all organisations equally. At an industry level:

- organisations in the finance and insurance industry are projected to be more likely than the average respondent to have made positive changes to their cyber security in the next 3 years – due to estimated volume and nature of AI systems that they use and deploy, which could be more valuable to a potential attacker
- the EU AI Act potentially appears to be a greater influence on organisations providing public services - those in public administration and defence and those in health were are perceived t be more likely than the average respondent to say the introduction of the EU AI Act is the most important factor (36% and 32% respectively, compared to 23%)
- organisations in finance and insurance; arts, entertainment, recreation and other services; wholesale and retail; education; health; and public administration and defence are estimated to be were more likely than the average respondent to have attributed all of the changes in their cyber security in the next 3 years to the EU AI Act (100%, 94%, 90%, 89%, 89% and 89% of respondents respectively)

When considered by special interest group:

- large businesses with complex and interconnected supply chains are estimated to be more likely to have made changes, particularly in relation to increasing their cyber security capacity and capability as a result of the EU AI Act than the average respondent
- • LAs/non-profit organisations providing important public services are projected to be more likely than the average respondent to have made changes and to rate 'the introduction of the EU AI Act' as the most important factor influencing these changes, which potentially indicates that the EU AI Act will have more of a potential impact on LAs/non-profits providing important public services than the average respondent
- large businesses are perceived to be more likely than the average respondent to have provided new and improved AI governance and specific cyber security training in the next 3 years, which indicates that the EU AI Act potentially leads to improved staff awareness and training within large businesses
- SMEs are estimated to be less likely to have made changes than the average respondent, which indicates that the EU AI Act will have less of an impact on SMEs than the average respondent
- MSPs were estimated to be less likely than other respondents to have changed their cyber security behaviour in the next 3 years, which indicates that the introduction of the EU AI Act potentially will have less of an impact on MSPs directly

These potential variations by industry and type of organisation highlight the value of providing more tailored guidance and support, that reflects their different influences and motivations, as well as more clearly linking security outcomes to business goals.

Part.2 Introduction

Purpose

AI & Partners used the findings of the Study to provide insight on the potential impact that the introduction of the EU AI Act may have on incentivising organisations across the UK and global markets to improve their cyber security outcomes. This report contains summarises of the findings that mirror those of Study in the context of the EU AI Act.

Terms of reference

AI & Partners required relevant benchmark research to deliver an initial understanding of the potential impact of the EU AI Act on organisational cyber security outcomes, including:

- a literature review of existing research in the subject area
- quantitative surveys of staff and Board members in a range of organisations to understand the potential impact that the EU AI Act can have on their cyber security outcomes
- qualitative interviews with staff and Board members to explore the findings of the quantitative survey in more detail

AI & Partners' stated key policy objectives for the latter part of the project were: to understand whether the EU AI Act can have an impact on organisational cyber security outcomes, whether potential improvements will be sustained and whether the EU AI Act may engender any unintended consequences.

The research requirements also include that any findings drawn from surveys should include a broad range of organisations including large businesses; large businesses with complex and interconnected supply chains; Managed Service Providers; and Local Authorities and non-profit organisations providing important or essential public services. In addition to this, it was decided that that the methodology should be designed to capture and incorporate the likely views of staff and Board members who are envisaged to be involved in the implementation of the EU AI Act, where possible.

Part.3 Potential Changes in Cyber Risk Management

Summary

The majority of organisations are likely to improve their cyber security measures. In the next 3 years, most organisations will increase the prioritisation of cyber security and investment in this area. They will introduce new or improved AI and cyber security policies, processes, procedures and technical controls. However, there will be a greater focus on governance, risk management, AI system security and system security than other aspects of cyber security.

This suggests that organisations are likely to benefit from improving their cyber resilience and the 'non-preventative' aspects of cyber security. It is potentially concerning, however, that a minority of organisations may not give cyber security the strategic focus required. Raising awareness of the business benefits of improved cyber security could help to address this issue.

Most organisations are expected to say that the changes made as a result of the EU AI Act will be sustained (84%). Further research is required to determine whether these likely changes will result in a longer-term behaviour change or a cultural shift towards more robust practices.

The Study indicates that organisations that had experienced a cyber security incident will be more likely to make improvements than those that had not experienced an incident. The same can be said for organisations that conduct a FRIA or those that deployed AI systems.

This indicates that more changes are going to be made in organisations where the EU AI Act was applicable. It also suggests that organisations that are not in scope of the regulations, or those that think they are not in scope, are likely to benefit from greater insights into real-life examples of the impact of a breach or encouraging the use of Business Impact Assessments and consideration of impact tolerances.

There is likely to be some variation in response by industry - organisations in the finance and insurance industry are anticipated to be more likely than other respondents to have made positive changes to their cyber security in the next 3 years. Interviewees are expect to say that this is due to the volume and nature of AI systems that they use, develop, market and/or deploy. This highlights the potential benefit of tailoring guidance and interventions by industry, taking account of differences in motivation and influences.

Findings in relation to potentially detrimental consequences of the EU AI Act are envisaged to be mixed. The majority of respondents are projected to not think that the EU AI Act will lead to excessive investment in cyber security (60%) or excessive focus on AI governance (54%).

However, a substantial proportion of respondents are anticipated to report these negative impacts (27% and 36% respectively). This indicates that organisations are likely to benefit from further guidance on the appropriate balance between AI governance and other aspects of cyber security

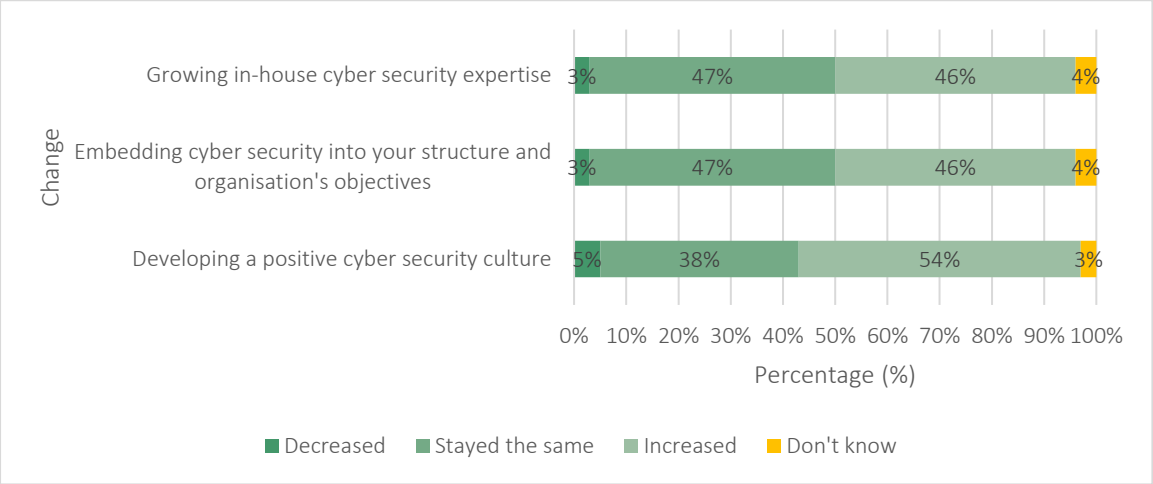
3.1 Context

3.1.1 Prioritisation of Cyber Security

Board Prioritisation

Approximately half of respondents to the Board survey (46%-54%) are likely to report an increase in the Board's prioritisation of the various aspects of cyber security governance in the next 3 years (see Figure 1). However, between 38% and 47% expect to say that it had remained the same.

Figure 1: Expected changes in Boards' prioritisation of cyber security governance in the next 3 years



Priority of policies, processes and procedures now compared to next 3 years

More respondents are expected to rate cyber security policies, processes and procedures as an even higher priority within their organisation in the next 3 years compared to today (see Figure 3.2). Fewer are expected to rate them as a lower priority in the next 3 years than today. The most common reason expected to be given by interviewees for this increase in priority is so that the organisation would be compliant with the EU AI Act. Another anticipated reason to be given by interviewees is that it is clear that cyber security risks are increasing, as more cyber-attacks are being reported.

Therefore, increasing the priority of cyber security policies, processes and procedures is necessary to increase their organisations' ability to protect themselves from a cyber-attack. Interviewees expected to report no change in priority potentially feel that they are – or are likely to be – mostly compliant compliant with the EU AI Act.

'Robust cyber security standards drives development of innovative AI use cases, Dr. Ilesh Dattani

AI in finance offers opportunities for fraud detection, risk assessment, and personalized services. The EU AI Act, aiming for secure AI, could bolster these benefits by requiring robust cybersecurity. However, overly strict security measures might hinder the agility needed for financial innovation.

Enforcing 'security by design – and by default'

"The EU AI Act enforces security by design for AI, potentially boosting cyber resilience across sectors from finance to manufacturing, but balancing security with innovation remains a challenge."

Dr. Ilesh Dattani, *CTO and Founder,* Assentian Limited

Figure 2: Anticipated priority of cyber security policies, processes and procedures (Now)

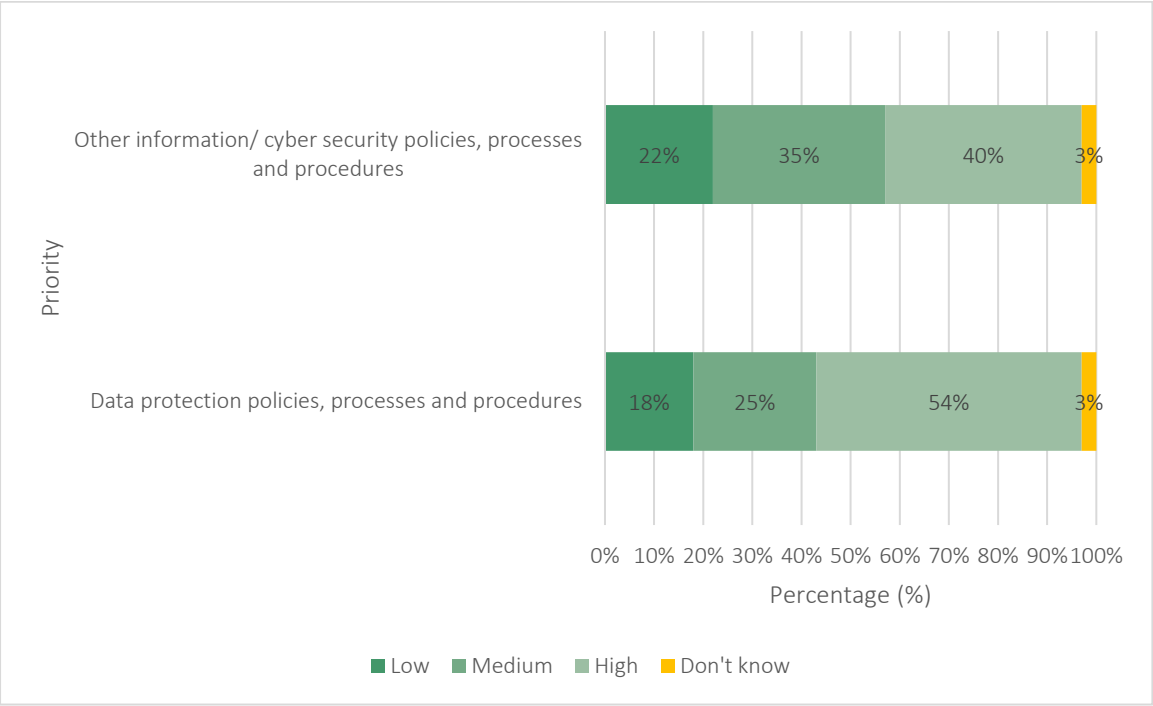
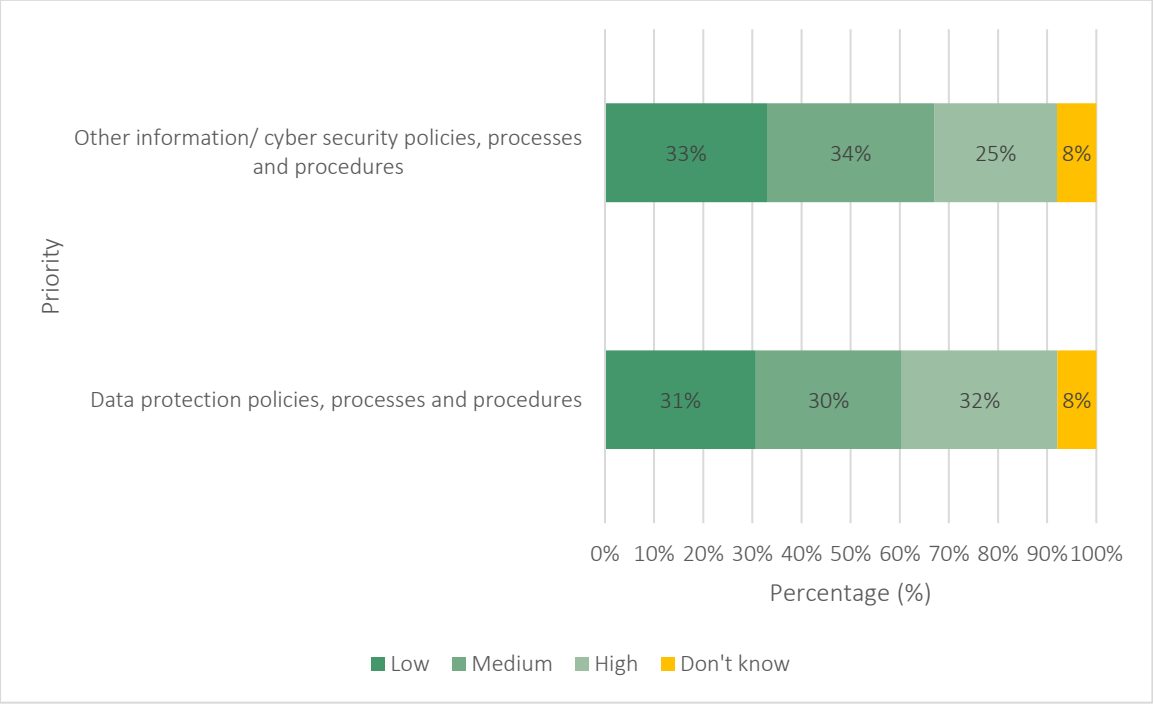


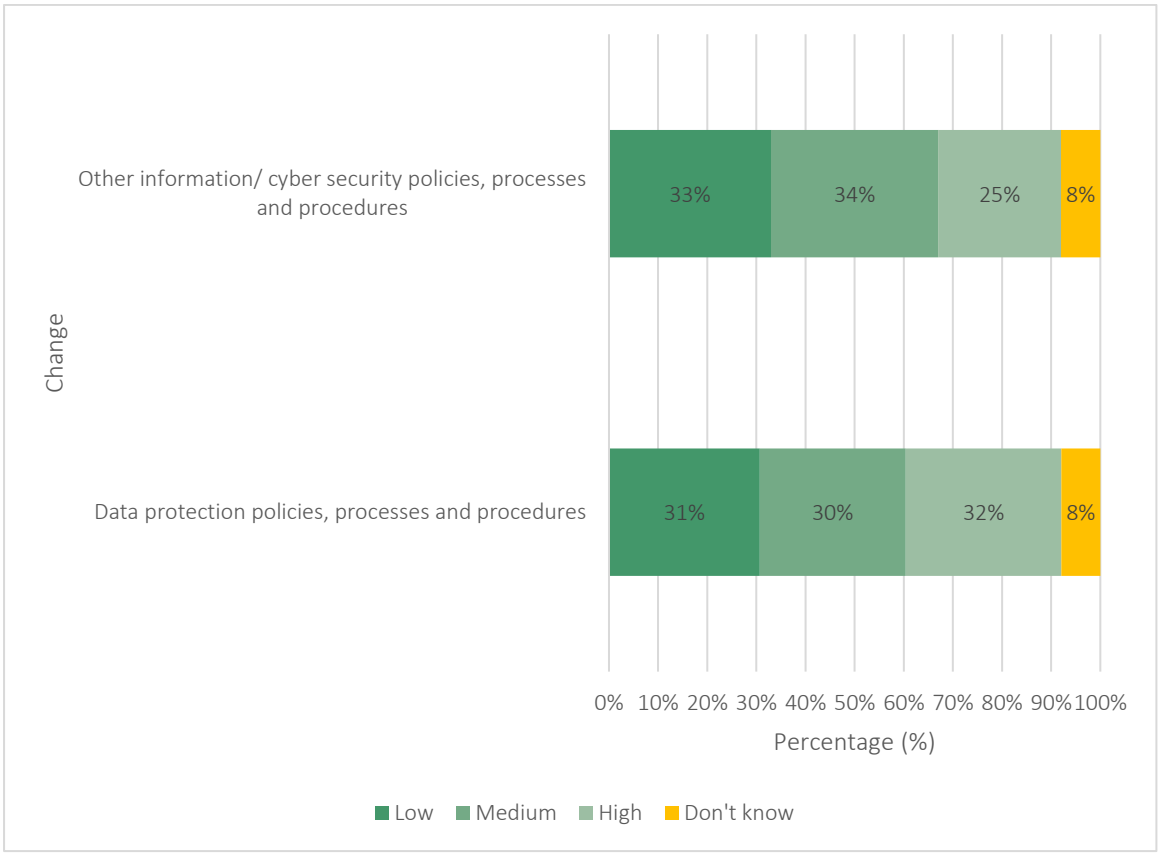
Figure 3: Anticipated priority of cyber security policies, processes and procedures (next three years)



3.1.2 Cyber security policies

In Figure 4, the majority of respondents are expected to say that their organisation has introduced and/or improved its AI policies (71%) and information security policies in the next 3 years (62%).

Figure 4: Envisaged changes in cyber security policies in the next three years



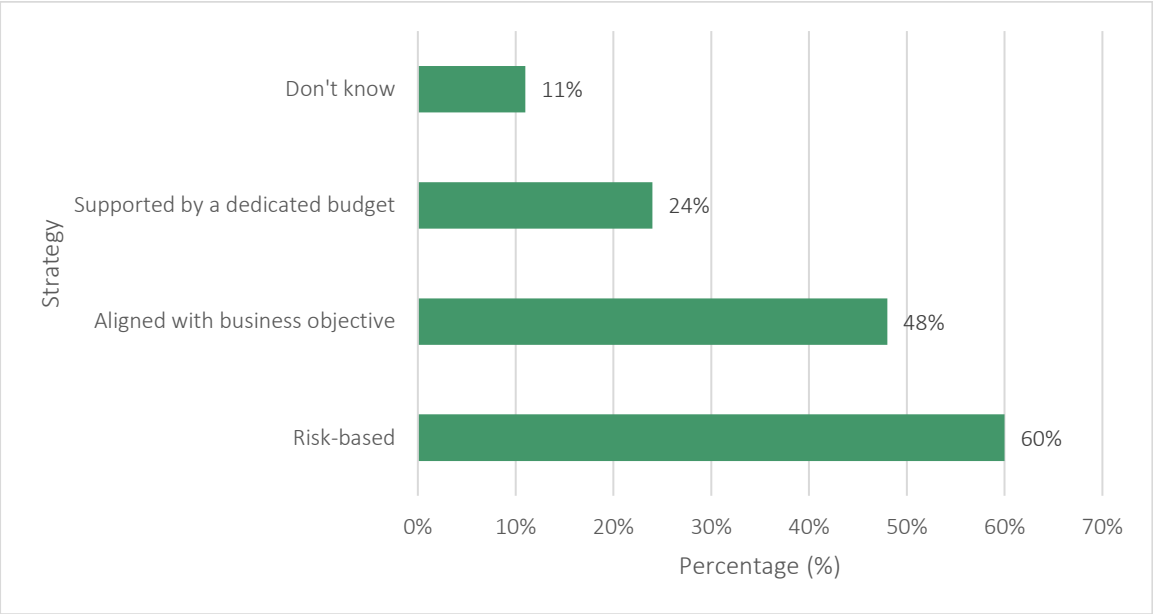
Board members are anticipated to be more likely to report changes to AI policies in the next 3 years than staff (79% anticipated to answer, 'introduced' and/or 'improved', compared to 69% of staff). Respondents who were IT or cyber security professionals are expected to be more likely to report changes in their information security policies than non-IT or cyber security professionals (70%, compared to 57%). Respondents who were not IT or cyber security professionals are expected to be less likely to report changes in their AI policies than the average respondent (69%, compared to 71%).

3.1.3 Cyber security strategy

Approximately a fifth of Board members are expected to say that their organisation has a dedicated cyber security strategy (18%) and approximately half have a cyber security strategy as part of their IT strategy (52%). It is concerning, however, that almost a third (31%) are expected to report having no formal cyber security strategy in place. We were unable to probe this projection further through the Study as all interviewees were from organisations with a formal strategy in place. This is potentially an area for further research.

Most of the organisations are expected to have a cyber security strategy in place, have a risk-based strategy (60%) and approximately half (48%) are anticipated to have a strategy that is aligned with business needs. Less than a quarter (24%), however, are envisaged to have a strategy that is supported by a dedicated budget. It is concerning to note that 11% of Board members are potentially unable to answer this question (said, 'Don't know').

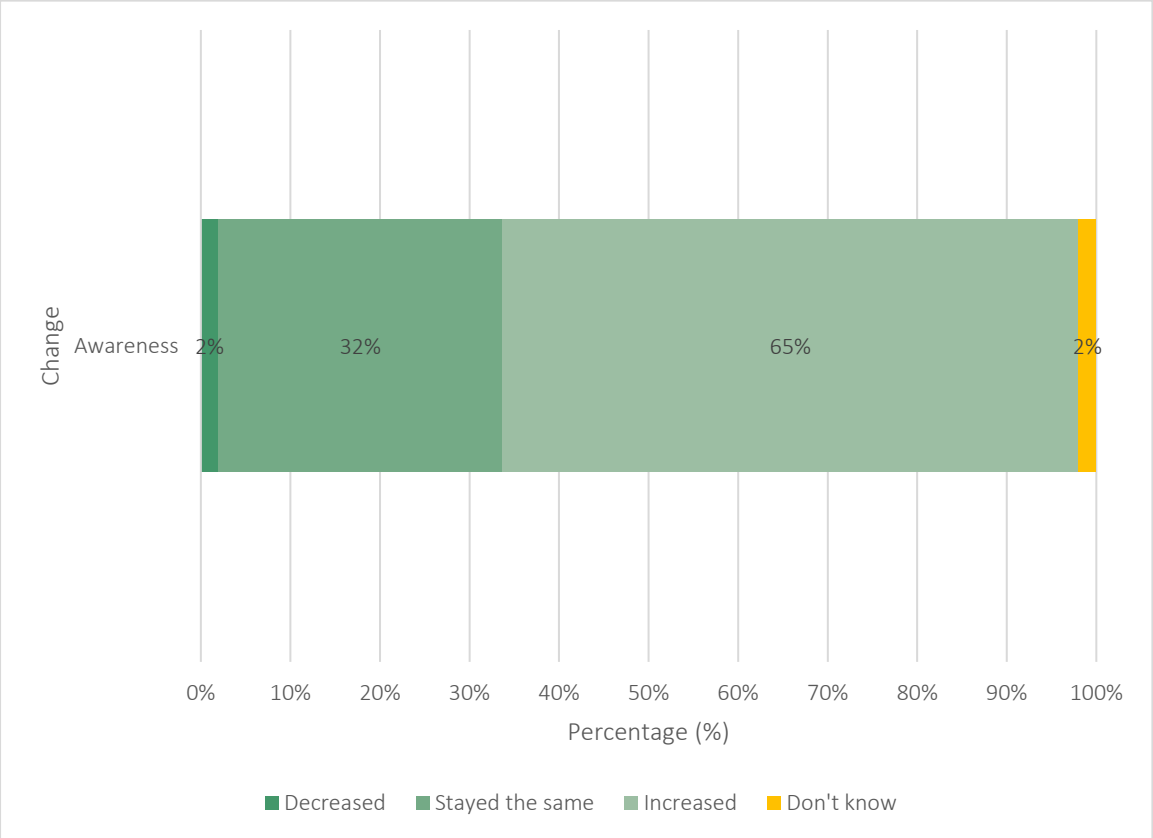
Figure 5: Expected proportion of cyber security strategies with the following key elements



3.1.4 Board level awareness

Most respondents (65%) are expected to say that their Board of Directors' awareness of cyber security will increase over the next 3 years, with a third (32%) anticipated to report that it will stay the same.

Figure 6: Anticipated change in Board of Directors' awareness of cyber security in next 3 years



‘GDPR experience helps strengthen cyber resilience’, Rialto

Leveraging GDPR experience, organizations can assess the EU AI Act's impact on cyber resilience by identifying compliance challenges, data protection protocols, and governance structures. This comparative analysis helps anticipate regulatory demands, enhance data security measures, and fortify cyber defenses across industries, ensuring robust adaptation to evolving AI-driven cyber threats.

Leverage GDPR experience to analyse EU AI Act’s Impact

“Our team of cybersecurity experts is at the forefront of understanding emerging threats. We're leveraging our GDPR experience to analyse the EU AI Act's impact on cyber resilience across industries. Join this white paper initiative to contribute to this critical research, especially in light of recent global IT disruptions.”

Richard Chiumento, *Director,* Rialto

rialto
ACCELERATED IMPACT

‘A significant step towards a safe digital future’, 300 Brains

In the wake of recent cyber incidents like the Crowdstrike attack, the EU AI Act's enforcement underscores the necessity for stringent cybersecurity measures. This legislation aims to enhance the security posture of all industry players, ensuring resilience against future threats.

Setting a robust framework for cyber security standards across industries

“The EU AI Act is a significant step towards a safer digital future, setting a robust framework for cybersecurity standards across industries.”

James Hodgson, *CEO,* 300 Brains

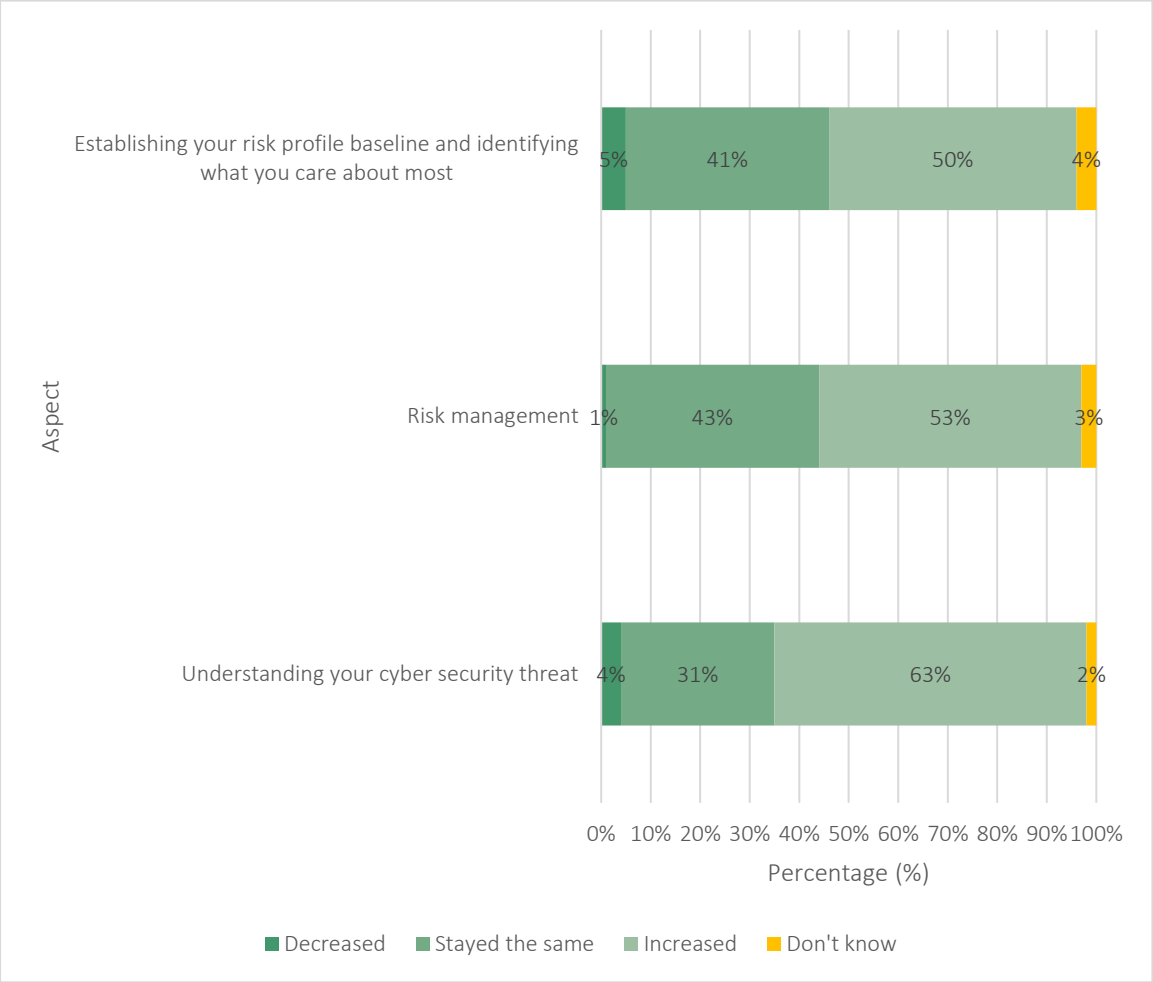
300 BRAINS | Do IT Smart

3.2 Risk Management

3.2.1 Prioritisation of risk management

Board members are expected to report an increase in the Board's prioritisation of risk management aspects of cyber security in the next 3 years.

Figure 7: Expected changes in board prioritisation of cyber risk management in the next 3 years



'EU AI Act to drive enhanced cyber risk management', AMLEGALS

The EU AI Act will drive enhanced cyber risk management through stricter compliance standards, requiring AI systems to undergo rigorous risk assessments, transparency measures, and monitoring. Organizations must bolster data protection protocols and ensure AI systems are robust, secure, responsible and accountable, mitigating cyber threats and aligning with new regulatory mandates.

AMLEGALS
LEGAL STRATEGISTS

‘Practical tools – prerequisite in meeting global expectations’, Netrascale

The recent CrowdStrike incident highlights the importance of consistent and actionable practices to ensure proactive and responsive capabilities. By prioritizing consistent and ego-free adherence to security protocols, controls, and practices, security practitioners can confidently meet global expectations and safeguard operations associated with their organization, partners, and clients.

The Critical Importance of Consistent Execution of Security Practices

Consistency in the execution of actionable processes, coupled with a strong and professional stance on risk management (technical, security, and business), forms the foundation of a proactive, responsive, and resilient security practice. Whether addressing regional issues like the Rogers Telecommunication incident in Canada, broad incidents such as the Swift outage that affected the Bank of England and the European Central Bank, or global failures like the recent CrowdStrike incident, these high-profile events underscore the critical importance of adhering to well-defined protocols and controls with risk tolerance supported by specific and actionable practices. At the same time, it is essential to support business empowerment, maintain a sustainable pace, and manage employee stress levels effectively.

A Spotlight on Effective Risk Management Strategies

Risk management plays a crucial role in setting actionable thresholds based on the likelihood of incidents (operational, business, resource, security, etc.). By assessing the probability and impact of potential threats, risk management frameworks enable organizations to prioritize their responses and allocate resources effectively. A structured approach, built upon the attitude of empowerment, helps ensure that significant concerns, errors, and omissions are addressed promptly, with appropriate mitigation strategies and tactics implemented. Threshold monitoring is used as part of the planning phase of an action and plays a critical aspect in monitoring the implementation, providing triggers that are executed (manually or through automation) when certain risks are identified, or levels are reached, allowing for a proactive rather than reactive security posture.

Simple and Consistent Practices and Controls

The effectiveness of risk management hinges on the consistent implementation of controls and practices across the entire organization. Mere documentation of policies is insufficient; they must be uniformly enforced and deeply embedded in its operational culture. For controls to be effective, it is essential to have a deep understanding of the implementation – it’s why, how, when, and where. Any control or practices, regardless of if it’s automated, procedural, or administrative needs to be defined and used consistently, in a direct and actionable manner that includes feedback that is executed against.

Risk Management and professional practices are sophisticated, and at the same time, simple. It is through these basic ideas that we support alignment and uniformity in an organization. In security, consistency and simplicity, which drives actionable matters builds operational resilience, proactive capabilities, confidence, and trust. These are measures that are not prohibitive but demonstrate a commitment to the protection of information and the execution of activities without disruption.

Flawed development practices, inadequate quality assurance, poor release management controls, insufficient focus-driven incident response preparation, and lack of phased rollouts are all common problems in large scale operational and security incidents. Each, a practice whose actual risk is quickly overlooked for speed of results. In their July 24, 2024, blog post, “Preliminary Post Incident Review (PIR): Content Configuration Update Impacting the Falcon Sensor and the Windows Operating System (BSOD),” CrowdStrike identified three practices that reflect upon the importance of adhering to and exploring supportive practices to reduce the opportunity for a critical event – each part of standards in operational, development, and security practices:

Comprehensive Testing including the use of local developer testing (unit testing), content update and rollback testing, stress testing, fuzzing, fault injection, stability testing, and content interface testing.

- Enhancing existing error handling and use of validation checks against changing expectations.
- Improved deployment practices including staggered deployment, improved monitoring, greater client-control of delivery mechanisms, and the use of release notes.
- Third party validation including independent code reviews and end-to-end reviews of quality and development processes.

Trust but verify?

As highlighted by CrowdStrike themselves, “trust but verify is obsolete.” Modern security is broad, an end-to-end identification of aspects that can impact availability, confidentiality, and integrity of the systems and the organization. Rather, contemporary practices must emphasize continuous verification and zero-trust to enhance the resilience and integrity of supply chains. Zero-trust is not just a buzzword but a pervasive concept! Risk management and core security practices themselves must move beyond "trust but verify" by embedding continuous verification into every aspect of the supply chain.

Empowering Proactive Risk Management

The NetraScale “SemanticRisk Adaptive Framework” is designed to be adaptive, leveraging advanced risk management techniques to ensure our clients can proactively identify and mitigate risks. As complexity of risk and regulation increases, building our solutions on this evolving framework means that we can offer unparalleled support in managing technical, security, and business risks. SemanticRisk is focused on not only empowering our clients to tackle current and future challenges, but also supporting them in achieving a sustainable and resilient operational pace. This framework is part of our corporate culture in fostering business empowerment while maintaining robust security practices and minimizing employee stress levels.

Concluding Thoughts

Consistent, actionable and specific practices, coupled with modern risk management should be part of an organization’s holistic approach. It is not just about security but operational capability that is embedded in the organizational culture. This cultural shift means that the ecosystem approach of thinking is integrated into every process, decision, and interaction across the value chain.

It involves educating employees about the values and principles of the practice and their role in maintaining cybersecurity and building resilience. Leadership must champion these values, demonstrating through policies and actions that security is a priority. By fostering a culture of consistent practices and continuous verification, organizations can ensure that every team member is vigilant and proactive, contributing to a robust security posture that protects against evolving threats.

Consistent & actionable practices key to mitigate risks

“Actionable practices are crucial in mitigating risks and empowering businesses. By consistently implementing clear and measured practices, organizations can improve operational resilience in an evolving threat landscape.”

Bryan Zarnett, *Chief Information Security Officer*, Netrascale

NETRASCALE

'Digital Twins for Enterprise – A New Approach to Enterprise Cyber/Tech Risk Management', EKAI

As enterprises increasingly rely on digital technologies, managing cyber and technology risks has become more complex. Traditional risk management approaches are often reactive and can be insufficient in addressing the dynamic nature of cyber threats. A promising innovation in this field is the application of 'Digital Twin' technology to enterprise risk management. This document explores the concept of Digital Twin, its application in cyber/tech risk management, and the benefits it offers to enterprises.

What is a Digital Twin?

A Digital Twin is a virtual replica of a physical object, system, or process. It allows for real-time monitoring, simulation, and analysis. In an enterprise context, a Digital Twin can represent the entire IT infrastructure, including hardware, software, and network configurations.

Key Components of a Digital Twin:

- Data Integration: Real-time data from various sources within the enterprise.
- Modeling and Simulation: Advanced algorithms to replicate the behavior and performance of the enterprise's digital ecosystem.
- Analytics: Tools to analyze data and provide insights for decision-making.

Traditional Enterprise Risk Management Approaches

Traditional risk management involves identifying potential risks, assessing their impact, and implementing measures to mitigate them. This approach has limitations:

- Static Assessments: Risk assessments are often conducted periodically, leading to outdated risk profiles.
- Reactive Measures: Responses to threats are typically reactive rather than proactive.
- Limited Scope: Traditional methods may not cover the full spectrum of cyber threats.

The Digital Twin Approach to Risk Management

Implementing a Digital Twin for enterprise risk management transforms the approach from reactive to proactive. The Digital Twin continuously monitors and analyzes the enterprise's digital environment, providing real-time insights and enabling dynamic risk management.

Benefits of Digital Twin in Risk Management:

- Real-time Monitoring: Continuous monitoring of the enterprise's IT infrastructure for potential threats.
- Predictive Analytics: Using historical data and machine learning to predict and mitigate risks before they materialize.
- Scenario Simulation: Simulating different risk scenarios to understand potential impacts and develop contingency plans.
- Holistic View: A comprehensive view of the enterprise's digital ecosystem, enabling a more integrated approach to risk management.

Implementing Digital Twin for Cyber/Tech Risk Management

Step 1: Data Collection and Integration

- Identify Data Sources: Gather data from all relevant sources within the enterprise, including network traffic, system logs, and user behavior.
- Data Integration: Use data integration tools to consolidate and normalize data for analysis.

Step 2: Building the Digital Twin

- **Modeling**: Develop a virtual model of the enterprise's IT infrastructure.
- **Simulation Tools**: Implement simulation tools to replicate the behavior of the digital ecosystem.

Step 3: Real-time Monitoring and Analysis

- **Monitoring Tools**: Deploy tools to monitor the Digital Twin in real-time.
- **Analytics**: Use analytics to identify anomalies, predict risks, and provide actionable insights.

Step 4: Continuous Improvement

- **Feedback Loop**: Implement a feedback loop to continuously update and improve the Digital Twin based on new data and insights.
- **Training and Adaptation**: Ensure the system adapts to new threats and changes in the IT environment.

Challenges and Considerations

Technical Challenges

- **Data Quality**: Ensuring the accuracy and completeness of data used to build the Digital Twin.
- **Integration Complexity**: Integrating data from diverse sources and systems.

Organizational Challenges

- **Change Management**: Managing the transition to a Digital Twin approach and ensuring stakeholder buy-in.
- **Skills and Expertise**: Developing the necessary skills and expertise to implement and maintain the Digital Twin.

The application of Digital Twin technology in enterprise cyber/tech risk management represents a significant advancement in the field. By enabling real-time monitoring, predictive analytics, and scenario simulation, Digital Twins provide a proactive and comprehensive approach to managing risks. While challenges exist, the potential benefits make it a compelling solution for modern enterprises seeking to enhance their risk management capabilities.

Proactive Cyber Risk Management via Simulation

"The unprecedented progress within AI technology has provided us with an opportunity to leverage GenAI to proactively predict and simulate severe but plausible threats to cyber security. Simulating the potential threats, lays the foundation of a future-ready enterprise."

Priya V Misra, *CEO*, EKAI

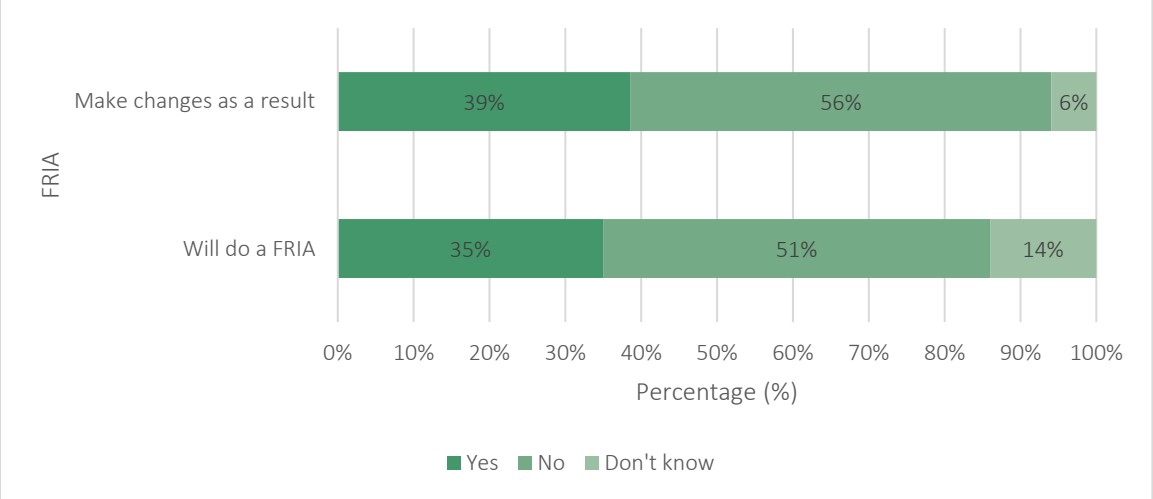
3.2.2 Fundamental Rights Impact Assessments ("FRIAs")

We also explore possible changes made as a result of having completed a FRIA as well as the rationale for not making changes. Approximately half of respondents to the survey (51%), are expected to say that their organisation will complete a FRIA, as required by the EU AI Act, where deployment of a high-risk AI systems is likely to result in a high risk to individuals' fundamental rights.

As can be expected, organisations that do deploy AI systems are expected to be more likely to conduct a FRIA (53%) than organisations that did not deploy a high-risk AI system (40%). It should be noted, however, that 75 of the 679 respondents that may complete a FRIA (11%) are expected to say that their organisation do not deploy high-risk AI systems.

IT or cyber security professionals are also expected to be more likely to say that their organisation will complete a FRIA (63%) than non-IT/cyber security professionals (47%). There was no statistically significant variation in the indicative responses of those that may have experienced a cyber security incident and those that had not.

Figure 8: Expected proportion of organisations who will conduct a FRIA in the next 3 years and make changes as a result



Cyber risk management a 'Key survival factor'

"Cyber criminals will use AI for cyber-attacks, so understanding cyber risk management and how to use AI to enhance cyber security is critical to stay ahead. Remember, the juicier the worm, the bigger the hook. In the AI age, cyber risk management will be the difference between success and failure - getting hooked by cyber criminals."

Doug Hohulin, *Business Associate*, AI & Partners

AI & Partners

Amsterdam - London - Singapore

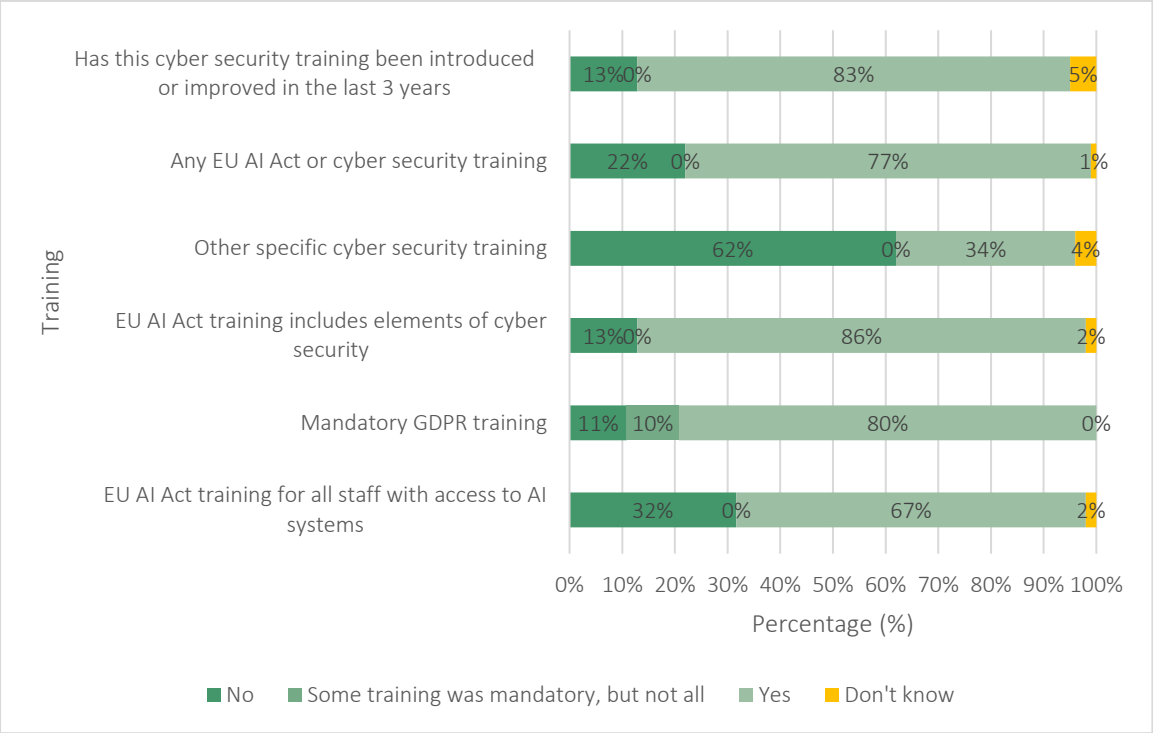
3.3 Staff Awareness and Training

3.3.1 Prioritisation of risk management

While 67% to the Study are expected to say that their organisation will provide training on the EU AI Act for all staff who had access to AI systems, almost a third (32%) are expected to have not.

Where EU AI Act training will be provided it is typically expected to be mandatory (80%) and generally included elements of cyber security (86%). For example, password protection, access control, patching and avoiding phishing. Most interviewees in the qualitative interviews are expected to said that they will provide training on the EU AI Act to all staff.

Figure 9: Expected training provided



'Weaknesses with a regulation-driven security risk management approach', 2021.AI

Management may focus overtly on strategy, policies and procedures. Instead of controls! No one can afford to wait years until controls are operationalized. Implement key controls immediately. Control your provider's restore procedures. Hack your LLM with a red team. Operationalize something now.

Operational risk controls – necessary for resilience

"Overreliance on a regulation-driven risk management approach which only focuses on strategy, policies and procedures may lead to a false sense of security. You need operational risk controls!)."

Neil Oschlag-Michael, *AI & Data Governance Advisor*, 2021.AI

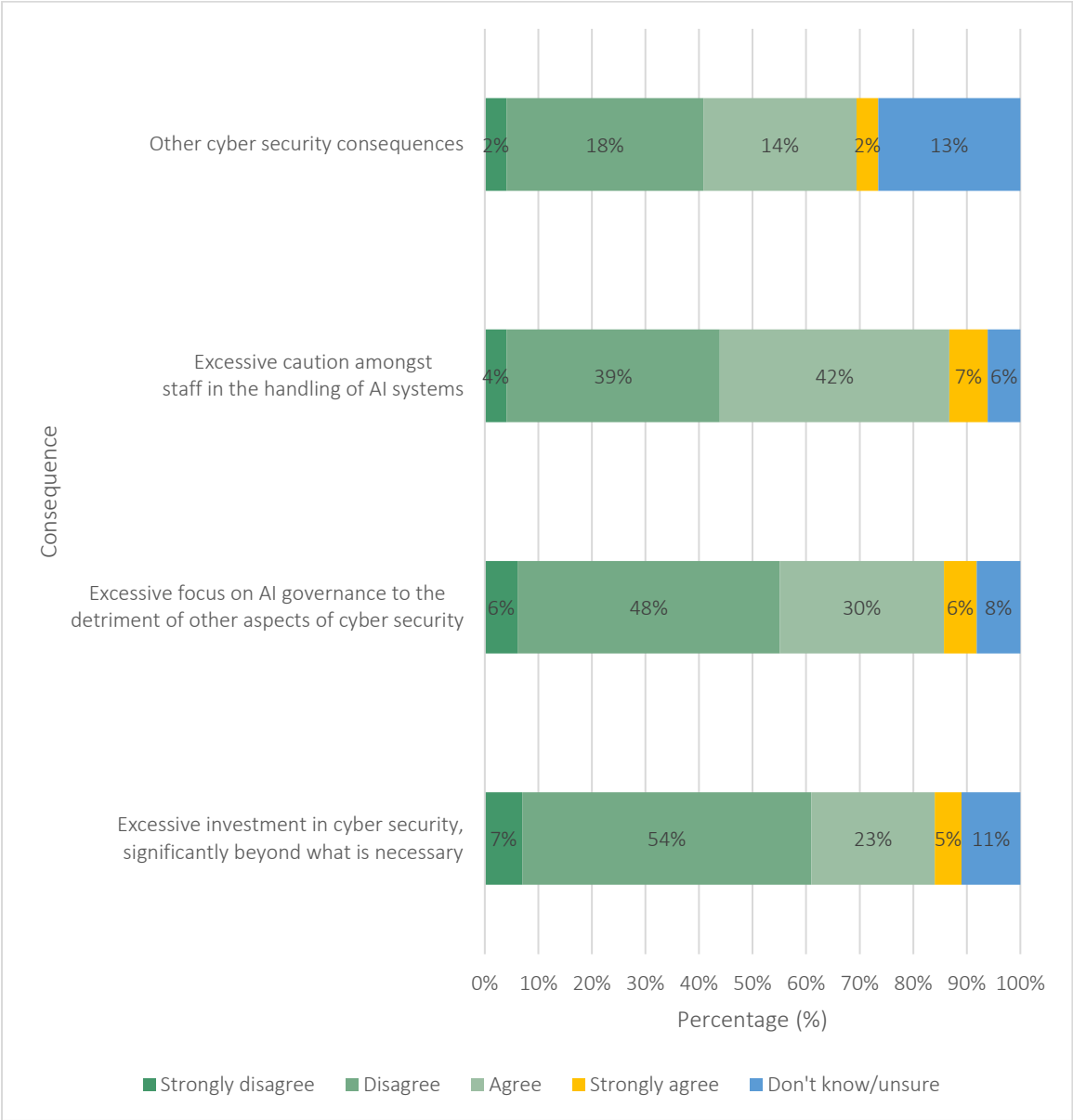
3.4 Unintended Consequences

Despite a very small proportion of respondents expected to report a decrease in the priority of various aspects of cyber security in the next 3 years, envisaged findings in relation to the potentially detrimental consequences of the EU AI Act are mixed. The majority of respondents are expected to disagree or strongly disagree that the EU AI Act will result in:

- excessive investment in cyber security, significantly beyond what is necessary (60%)
- excessive focus on AI governance to the detriment of other aspects of cyber security (54%)

However, a substantial proportion of respondents are anticipated to agree or strongly agree with these statements (27% and 36% respectively). The proportion of respondents who are expected to agree and disagree that the EU AI Act will lead to excessive caution amongst staff in the handling of AI systems was approximately 50:50 (including those who strongly agreed or strongly disagreed). Some interviewees are expected to report that the changes made as a result of the EU AI Act will not improve their organisation's ability to protect themselves against a cyber-attack.

Figure 10: Other potential consequences of EU AI Act



Excessive focus on AI governance

Organisations that had not experienced a cyber security incident (58%) are expected to be more likely than those that had (36%) to disagree or strongly disagree that the EU AI Act will lead to excessive focus on AI governance to the detriment of other aspects of cyber security. Respondents who were not IT or cyber security professionals are also expected to be more likely to disagree or strongly disagree (60%) than IT or cyber security professionals (38%). Respondents in public administration and defence (69%) and arts, entertainment, recreation and other services (81%) are anticipated to be more likely to have disagree or strongly disagree that the EU AI Act will lead to excessive focus on AI governance to the detriment of other aspects of cyber security, than those in the production industry (36%).

Data protection concerns drive renewed focus on cyber security

"Private banks, wealth managers and family offices in Europe must keep cybersecurity uppermost in their minds, particularly because users of these institutions hold considerable fortunes, hold prominent positions in business, and closely value their privacy. Data protection is at the centre of what guarding clients' financial and non-financial affairs is all about. With AI developing rapidly, it has potential not just to cause new problems if it used carelessly, but also to solve them too."

Tom Burroughes, *Group Editor*, WealthBriefing

Regulation of cyber security AI systems helps preserve financial stability

"Enhancing cyber resilience in an AI era will unquestionably be at the top of the agenda for financial institutions across the globe. The recent CrowdStrike incident further emphasises the need for robust regulatory frameworks to help foster greater regulation of cybersecurity systems, as well as AI systems in general. This is the only way to protect both businesses and consumers, and ultimately to preserve financial stability.

"The rise of GenAI has magnified the risks of sensitive information exposure, becoming a compliance nightmare almost overnight. Ultimately, the best safeguard against this risk is to build appropriate governance processes around any GenAI model in production, whether built in house or from third party vendors. We must ensure that we do not adopt GenAI for its own sake, and that when it is adopted, human-in-the-loop evaluation and monitoring systems are put in place."

Dr. Yin Lu, *Global Head of AI and Product*, CUBE

Part.4 Likely Driving Factors

Summary

EU AI Act is expected to be considered the most important factor driving change in cyber security in the next 3 years:

- 23% of all respondents to both surveys are anticipated to name the introduction of the EU AI Act the most important factor
- 19% are anticipated to say that they have a desire to comply and avoid penalties

This is supported by the findings of the Study. Increased awareness of the financial (5%) and reputational (5%) costs of cyberattacks were the next most popular responses.

Respondents that had experienced an incident are expected to be more likely than those that had not to state that 'perceived, heightened external threat of cyber-attacks in their industry' had influenced changes in their cyber security in the next 3 years (34%, compared to 27%). While respondents that will complete a FRIA or that deployed, developed, marketed and/or used AI systems are expected to be more likely than those that will not do a FRIA or do not deploy, develop, market and/or use AI systems to cite a range of factors, indicating a potential higher level of awareness of the diverse range of factors.

The vast majority of respondents are expected to say that the EU AI Act has influenced all of the changes in their organisation's cyber security over the next 3 years, at least to a small extent (82%). This is expected to be more common amongst respondents that will complete a FRIA, experienced a cyber security incident or deployed, developed, marketed and/or used AI systems than those that had not.

4.1 Potential Range of Factors

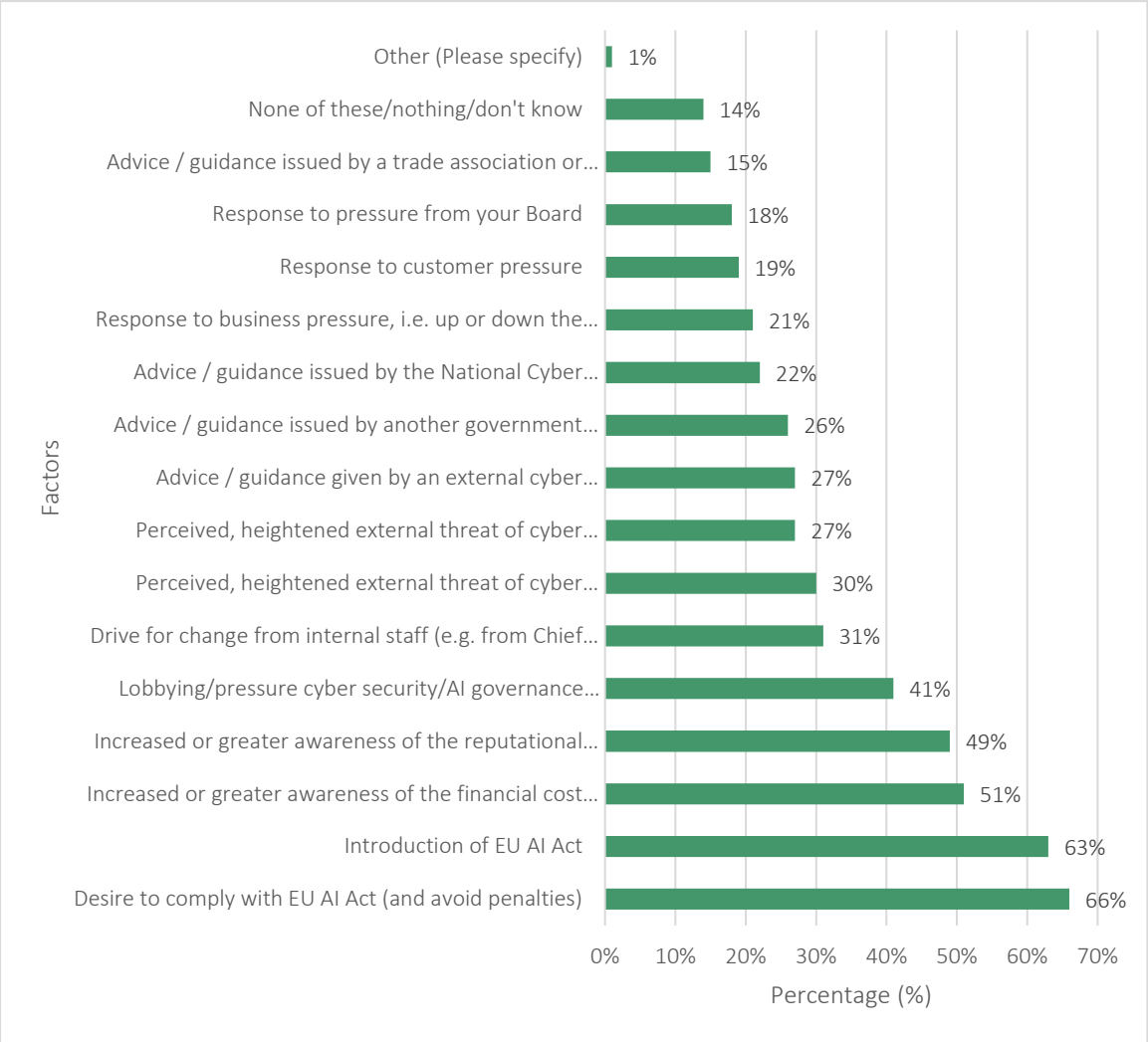
In regards to what factors will specifically influence cyber security changes over the next 3 years, the majority of respondents are expected to link to the GDPR. Desire to comply with the EU AI Act and avoid penalties is envisaged to be the most popular response (66%), followed by the introduction of the EU AI Act generally (63%). Increased or greater awareness of the financial cost (51%) and reputational cost (49%) of serious incident breaches or cyber-attacks are expected popular responses.

The vast majority of interviewees are expected to say that they were motivated to make changes to their cyber security by the EU AI Act, as well as other factors. This highlights that regulation is set to play a key part in the multiple factors that influence organisations' behaviour. The other factor expected to be cited by interviewees is awareness of the increasing prevalence of cyber-attacks.

Other likely factors to be mentioned by interviewees include:

- regular reviews of their cyber security which highlighted areas for improvements
- new technology to support and enable that change, for example Cloud storage, which made it easier for them to store personal data securely
- outsourced cyber professionals highlighting the need to improve cyber security policies and processes
- increasing client base/increase in the number of clients who expected compliance with the EU AI Act
- previous experience of a cyber incident
- increased frequency of flexible and remote working

Figure 11: Likely factors to influence these changes



'Organisations will be compelled to take action to reinforce cybersecurity controls', Cyber Security Unity

With information terms of literature on the potential impact of the EU AI Act being scares, this report is much needed and covers the impact of the EU AI Act on individual countries. Definite conclusions on their impact on individual countries, included the United Kingdom ("UK"), specifically cannot be drawn from any existing research. It is clear that most organisations are likely to improve their cyber security when measured against relevant standards, and this report will go into how they can do this.

Need for stringent regulatory measures to prevent cybersecurity-related incidents

"I'm delighted to take part in this report, it highlights the urgent need for stringent regulatory measures, risk management, transparency, and accountability in AI systems to prevent incidents such as the CrowdStrike global IT outage."

Lisa Venture MBE, *Founder*, Cyber Security Unity

‘Article 15 sets the benchmark for high-risk AI systems’, Access Partnership

The EU AI Act’s Article 15 mandates robust measures for high-risk AI systems, including technical redundancy and fail-safe plans. This enhances cybersecurity, ensuring systems are resilient against faults. Considering the CrowdStrike global outage incident in July 2024, these provisions prevent monopolistic vulnerabilities, bolster industry-wide competitiveness, and secure critical infrastructures.

EU AI Act – A crucial step forward for securing our digital future

“The EU AI Act marks a crucial step towards securing our digital future, ensuring robust, resilient AI systems that enhance cybersecurity and foster fair competition across industries.”

Mark Smitham*, Senior Manager*, Access Partnership

4.2 Most Important Factor

If asked what the most important factor is, introduction of the EU AI Act (23%) and the desire to comply with it and avoid financial penalties (19%) is expected to come top. Over a quarter of respondents are expected to say that all factors were important and that they are unable to choose (26%).

Staff are expected to be more likely than Board members to rank ‘introduction of the EU AI Act’ as the most important factor influencing cyber security changes (24% of staff, compared to 14% of Board members).

While Board members are anticipated to be more likely than staff to have said that they were unable to choose one factor as the most important factor (39% of Board members compared to 24% of staff). Respondents that conduct a FRIA are expected to be more likely to have said ‘introduction of the EU AI Act’ as the most important factor influencing changes to cyber security than the average respondent (26%, compared to 23% of respondents, respectively).

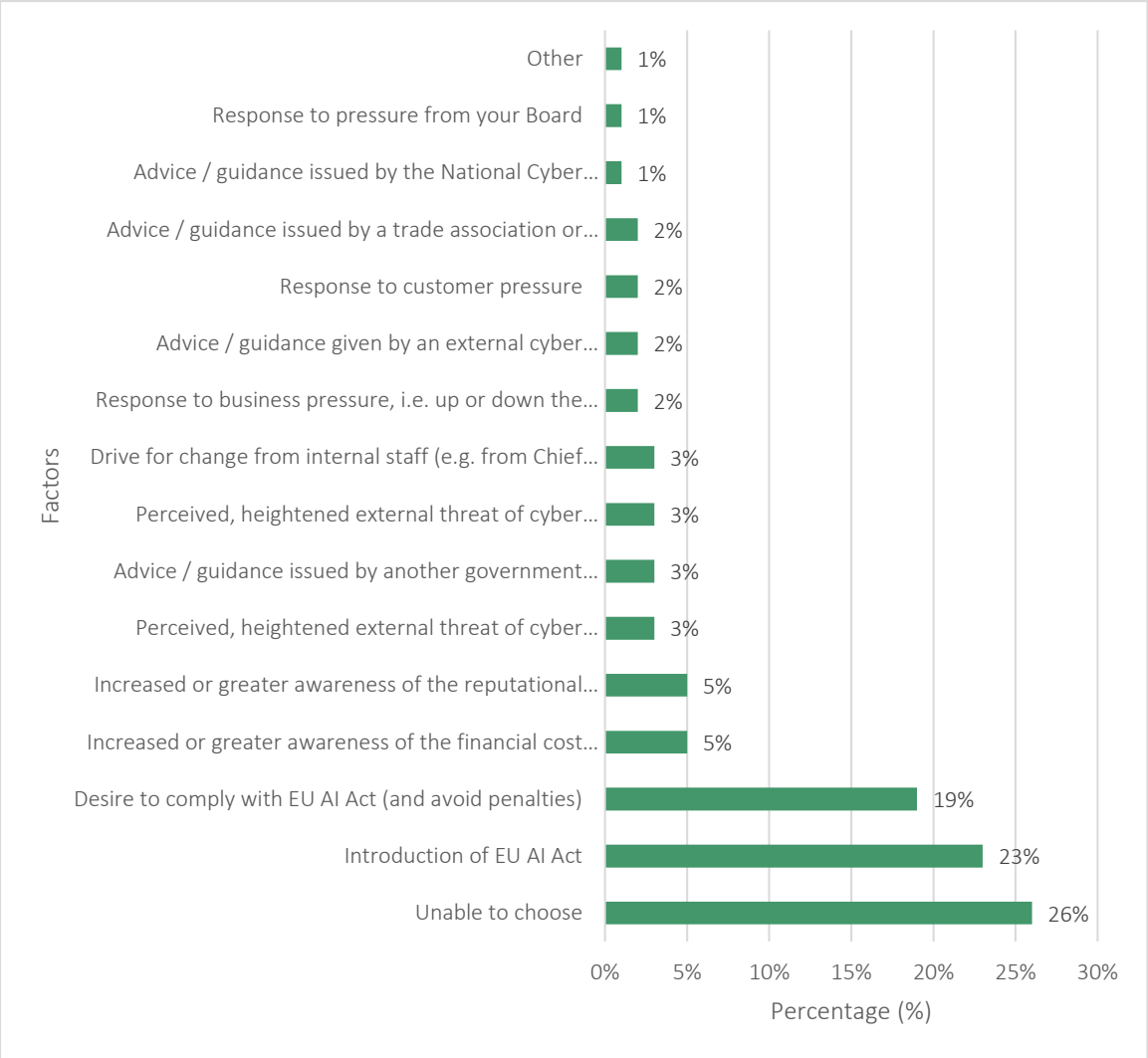
Respondents who were cyber security or IT professionals are expected to be less likely to have said that either ‘introduction of the EU AI Act’ (18%) or ‘desire to comply with the EU AI Act and avoid penalties’ (12%) as the most important factors influencing cyber security changes than those who were not cyber security or IT professionals (27% and 21% respectively), possibly because they were more likely to have cited a range of other external factors as drivers.

Respondents expected to have not experienced a cyber security incident (21%) are envisaged to be more likely than those who had (10%) to cite ‘desire to comply with the EU AI Act and avoid penalties’ as the most important factor. They are also anticipated to be more likely to have said that they could not choose one factor as the most important (28%, compared to 17%).

When considered by industry, respondents in public administration and defence (36%) and the health industry (32%) are anticipated to be more likely than other respondents (23%) to have cited ‘introduction of the EU AI Act’ as the most important factor.

Respondents in the information and communication industry (9%) are expected to be less likely than the average respondent (19%) to have stated that ‘desire to comply with the EU AI Act and avoid penalties’ as the most important factor.

Figure 12: Likely factors ranked as the most important in influencing these changes



'AI innovation shifts focus back to cyber security', gunnercooke

Cybersecurity has long been an issue across all industries. However the innovation of AI forces a refocussing on ensuring cybersecurity, being ironically both catalyst to facilitate better security and a mechanism for undermining the systems and controls firms have in place to keep themselves secure.

AI's value contingent on perception of being safe

"Whilst cybersecurity may be becoming one of the golden oldies of potential risk, recent events have reinforced just how vital it is to get correct. Use of AI needs to be cognisant of this, as AI's value is contingent on its perception as being safe to use from a security perspective."

James Burnie, *Partner*, gunnercooke

gunnercooke

4.3 Influence of EU AI Act

If asked to what extent all of the changes in their organisation's cyber security will be as a result of the introduction of the EU AI Act as opposed to other factors, it is expected:

- the majority of respondents will answer to a small or some extent (56%)
- a further quarter will say to a great or very great extent (26%)
- only 15% of respondents will say that the changes made were not a result of the introduction of the EU AI Act

There is likely some variation in response by industry and type of respondent. Where these variations were statistically significant, they are summarised below.

Respondents that conduct a FRIA, experienced a cyber security incident or developed, deployed, used, and/or marketed AI systems are expected to be more likely to have attributed all changes to the EU AI Act than those that had not completed a FRIA or developed, deployed, used, and/or marketed AI systems (90%, 90% and 87% answered at least 'to a small extent,' compared to 72% and 62% respectively). Respondents who were cyber security or IT professionals are expected to also be more likely to attribute all changes to the EU AI Act than non-cyber security or IT professionals (86% at least 'to a small extent,' compared to 80%).

Respondents in: finance and insurance; arts, entertainment, recreation and other services; wholesale and retail; education; health; and public administration and defence are expected to be more likely than the average respondent to attribute all of the changes in their cyber security over the next 3 years to the EU AI Act (100%, 98%, 94%, 90%, 89%, 89% and 89% answered at least 'to a small extent,' respectively, compared to 82% of all respondents to both surveys).

We also explored the potential extent to which the EU AI ACT had influenced changes to individual aspects of cyber security.

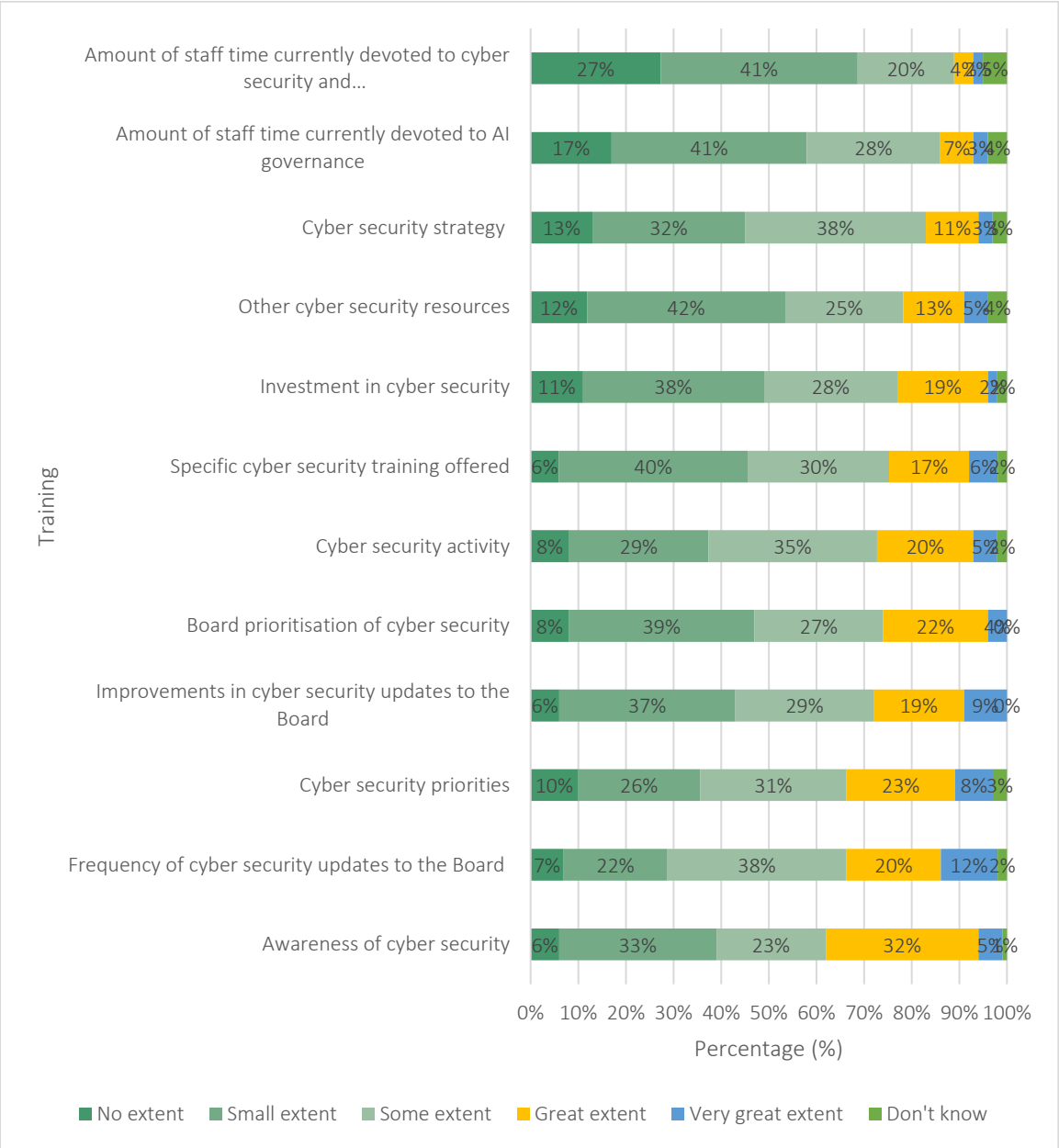
The majority of respondents are expected to report that the introduction of the EU AI Act will influence the changes reported in their cyber security in the next 3 years, to at least a small extent.

The changes most likely to be influenced by the introduction of the EU AI Act to a great or very great extent are likely to be:

- Board's awareness of cyber security (37%)
- Frequency of cyber security updates to the Board (32%)
- Cyber security policies (31%)

The amount of staff time are expected to devote to AI governance and cyber security and information security are expected to be the least likely to be influenced to by the introduction of the EU AI Act, i.e. respondents are more likely to have responded 'no extent' (17% and 27% of respondents to the staff survey answered 'no extent' respectively). There is expected to be some variation in response by industry and type of respondent.

Figure 13: Extent to which the following changes are expected to be influenced by the EU AI Act



EU AI Act helps protect AI against evolving cyber threats

"Cybersecurity in the age of AI isn't just an option—it's a necessity. The EU AI Act drives organizations to bolster their cyber defences and governance and ensures AI systems and their supporting data are safeguarded against evolving threats."

Helen Yu, *CEO*, Tigon Advisory Corp

Tigon Advisory

Start-ups, cure your disconnects.

‘Data governance backbone of secure data management platforms’, KATLAS Technology Limited

Building a secure data management platform for industrial research using artificial intelligence is a complex task. It must ensure compliance with GDPR and protect against quantum computing attacks. To succeed, we need a modular platform that allows us to dynamically update encryption libraries. This means any encryption module, using agreed-upon standards and desired cryptography technology, can be easily integrated.

Key lies in trusted, self-controlled digital identities

“Government agencies and corporations use Privacy Enhancing Technologies (PETS) as a covert way to gather personal data without our permission. But the key to harnessing AI's power lies in trusted, self-controlled digital identities.

“KATLAS revolutionizes data sharing and governance. Founded in 2019, it empowers users with smart wallets and agents to build verifiable digital profiles. The platform hosts off-chain digital twins, connecting via smart contracts with privacy protocols on a decentralized foundation. Interoperable with legacy systems, KATLAS enhances security and incentivizes participation.”

Edward Cole, *CEO*, KATLAS Technology Limited

KATLAS
Distributed Governance

Central banks recognise increasing importance of firms’ cyber resilience

“The development of artificial intelligence (AI) tools and their integration into the financial market present new opportunities; however, they also escalate the risk of cyberattacks. This issue is particularly pertinent for central banks, which are responsible for market oversight, the consolidation of large volumes of sensitive data, and the provision of the necessary infrastructure for the financial market’s operation. Consequently, the implementation of additional security measures has become imperative. Regulators are now contemplating a revision of existing regulatory frameworks in response to the escalating risks. Potential solutions include the enhancement of current resilience practices and standards, as well as the adoption of AI-driven solutions for platforms that analyse cyber incidents. These platforms could facilitate the exchange of information on cyber incidents among market participants and coordinate efforts to mitigate ongoing cyberattacks. Such platforms could originate from regulatory initiatives or result from collaborations with relevant market associations.”

Kate Shcheglova-Goldfinch, *AI-governance and regulatory expert*

Important to create awareness around cybersecurity

“The report covers how the EU AI Act may create awareness about cybersecurity issues and gets into granularity about how different stakeholders in the ecosystem may respond to the EU AI Act for their cybersecurity preparedness. The broad conceptual comparison drawn between the EU AI Act and the GDPR is equally fascinating.”

Vibhav Mithal, *Associate Partner*, Anand and Anand

‘Data governance backbone of secure data management platforms’, Dr. Indranil Nath, CEng, FIoD, FBCS, CITP, PSM

The EU AI Act mandates embedding cybersecurity from the design phase, enforcing stringent risk management for high-risk AI systems. It emphasises incident reporting, continuous monitoring, and professional training. The Act focuses on data protection, rapid restoration processes, and managing third-party risks to ensure a resilient digital ecosystem and build public trust.

Implications for Cybersecurity in the Context of the EU AI Act

The EU AI Act underscores the necessity of embedding cybersecurity measures from the design phase, mandating stringent risk management and compliance for high-risk AI systems. It emphasises the importance of incident reporting, continuous monitoring, and managing third-party risks to ensure transparency and resilience. The Act highlights the critical need for professional training, advocating for qualified cybersecurity experts to protect systems and build public trust. Additionally, it focuses on data protection and rapid restoration processes, which are essential for maintaining robust and resilient AI and IT infrastructure. The Act aims to secure AI systems and critical infrastructure by implementing these measures, ensuring a trustworthy and resilient digital ecosystem.

The EU AI Act emphasises the critical need for robust cybersecurity measures integrated by design and enforced through strong governance and regulation.

Critical Implications for Cybersecurity:

1. Mandatory Governance and Accountability:
   - EU AI Act: High-risk AI systems require stringent risk management and compliance measures.
   - Recommendation: Advocate for a compulsory Cybersecurity Governance Code, holding company boards accountable for cybersecurity.
2. Security by Design and by Default:
   - EU AI Act: Security must be embedded in AI systems from the outset.
   - Recommendation: Enforce a 'secure and resilient by design' culture for all critical IT systems.
3. Incident Reporting and Transparency:
   - EU AI Act: Requires incident reporting for high-risk AI systems to relevant authorities.
   - Recommendation: Call for mandatory breach reporting and quarterly risk assessments, including third-party risks.
4. Continuous Monitoring and Assurance:
   - EU AI Act: Ensures ongoing evaluations of cybersecurity measures.
   - Recommendation: Promote continuous monitoring, particularly in government and critical national infrastructure supply chains.
5. Professional Training and Awareness:
   - EU AI Act: Emphasises the need for qualified cybersecurity professionals.
   - Recommendation: Suggest increased investment in cybersecurity training and a government-led awareness campaign.
6. Supply Chain Security:
   - EU AI Act: Providers must manage risks associated with third-party components.
   - Recommendation: Continuous monitoring and assurance of third parties are crucial, especially in critical infrastructure.

7. Data Protection and Privacy:
   - EU AI Act: Reinforces data protection measures.
   - Recommendation: Highlight the importance of reliable backups and quick restoration processes.

8. Building Public Trust:
   - EU AI Act: Promotes transparency and accountability to build trust in AI systems.
   - Recommendation: Support professional registrations and Chartered status for cybersecurity practitioners to enhance public trust.

Figure 14: Critical implications for cybersecurity

Embedding 'cyber security by design'

"Embedding cybersecurity by design and enforcing strong governance, the EU AI Act ensures resilient AI systems, protects critical infrastructure, builds public trust in a secure digital ecosystem, and mandates corporate director responsibility."

Dr. Indranil Nath FIoD, FBCS, CEng, CITP, *Honorary Senior Visiting Fellow,* City University of London

‘Regulatory shift driving renewed cyber focus’, QX Lab AI

With the EU AI Act coming into force, organizations must prioritize cyber security to mitigate risks associated with AI systems. This regulatory shift necessitates a comprehensive approach to cyber risk management, including enhanced policies, technical controls, and ongoing Board-level awareness. Our commitment to these standards ensures a secure and resilient AI infrastructure.

Enterprises must safeguard their systems and data

"The introduction of the EU AI Act will undoubtedly drive significant improvements in cyber security, encouraging organizations to adopt more robust policies and procedures to safeguard their AI systems and data."

Arjun Prasad, *Co-Founder and Chief Strategy Officer,* QX Lab AI

‘Enterprises urged to reinforce their AI Governance and cybersecurity practices’, Unicsoft

To comply with EU AI Act regulations companies will need to step up their AI governance and cybersecurity efforts. Drawing on the expertise of software development and consulting professionals can help make the transition smoother enabling businesses to meet requirements while also seizing opportunities for innovation and bolstered security.

Enterprises encouraged to uptake innovative AI

“The EU AI Act enforces standards for AI and cybersecurity urging companies to embrace technologies. It highlights the need for expert advice in following regulations and making use of progress.”

Tomasz Kęczkowski, *Director of Business Development,* Unicsoft

Part.5 Caveats to the Report

There are inherent limitations to the Report that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most ex-ante based research reports based on forthcoming legislation.

- Divergence in Regulatory Intent: While the GDPR may share similarities with the EU AI Act, it is essential to recognize potential differences in regulatory goals and objectives. Variances in legislative intent or policy priorities could lead to divergent outcomes despite surface-level similarities.
- Contextual Disparities: The socio-economic, political, and cultural contexts surrounding the GDPR and EU AI Act are likely to differ significantly. These contextual variations can influence stakeholder behaviour, enforcement mechanisms, and overall regulatory effectiveness, thereby impacting the validity of direct comparisons and inferences.
- Evolution of Stakeholder Dynamics: Stakeholder dynamics, including the composition, interests, and influence of relevant parties, may have evolved between the implementation of the GDPR and the EU AI Act. Changes in stakeholder engagement strategies or power dynamics can alter the regulatory landscape and its outcomes.
- Methodological Limitations: Any inferences drawn from the Study must be tempered by an acknowledgment of its methodological limitations. Factors such as sample size, research design, data quality, and the generalizability of findings could impact the reliability and applicability of conclusions to the current EU AI Act regulatory environment.
- Unforeseen External Factors: External variables that were not accounted for in the Study may exert significant influence on the outcomes of the EU AI Act. These could include technological advancements, shifts in market dynamics, or unforeseen events such as global pandemics, all of which may shape regulatory implementation and outcomes in unforeseen ways.
- Dynamic Regulatory Environment: Regulatory frameworks are subject to continuous evolution and adaptation in response to changing societal needs, political priorities, and emerging challenges. Therefore, while insights from the GDPR can provide valuable guidance, it is imperative to recognize the dynamic nature of regulatory environments and exercise caution when extrapolating findings to inform future regulatory decisions.

Annex A – EU AI Act GDPR Equivalents: Actors

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 5: Comparison between EU AI Act and GDPR in terms of in-scope actors

EU AI Act	GDPR	Comment
Provider	Data Controller or Data Processor	The 'provider' under the EU AI Act is akin to both 'data controller' and 'data processor' in GDPR. A 'data controller' determines the purposes and means of processing personal data, while a 'data processor' processes personal data on behalf of the controller. Both roles involve developing, deploying, or operating systems AI systems in the EU AI Act and data processing systems in GDPR) under their authority.
Deployer	Data Controller	The 'deployer' in the EU AI Act closely resembles the 'data controller' in GDPR, as both are entities that use the system (AI or data processing) under their authority for specific purposes, except for personal or household activities.
Authorised Representative	Concept of Representation	The concept of an 'authorised representative' in the EU AI Act, who acts on behalf of a provider, is somewhat mirrored in GDPR by the requirement for non-EU entities to appoint a representative within the EU to interact with supervisory authorities and data subjects.
Importer	Concept of Representation or Data Importer	The 'importer' role, specific to bringing AI systems from outside the EU into the Union market, can be loosely compared to GDPR's concept of data importers or representatives of non-EU data controllers/processors who must ensure compliance with EU data protection standards when importing data.
Distributor	No direct equivalent	The 'distributor' role in the EU AI Act, which involves making AI systems available on the Union market, does not have a direct equivalent in GDPR. However, any entity involved in the distribution chain could be considered a data processor if they process personal data on behalf of a data controller.
Operator	Data Controller or Data Processor	The 'operator' encompasses several roles (provider, product manufacturer, deployer, authorised representative, importer, or distributor) in the EU AI Act, similar to how both 'data controllers' and 'data processors' cover various entities involved in data handling under GDPR.

Annex B – EU AI Act GDPR Equivalents: Activities

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 6: Comparison between EU AI Act and GDPR in terms of in-scope activities

EU AI Act	GDPR	Comment
Making available on the market	Data processing	Akin to the GDPR's concept of 'Data Processing'. While the EU AI Act discusses the supply of AI systems for commercial activity, GDPR regulates the processing of personal data, which can include the distribution or use of data processing systems or services.
Putting into service	Data Collection and Use	Resembles the GDPR's 'Data Collection and Use'. This term refers to the initial use of data or systems for processing personal data, aligning with the GDPR's focus on how personal data is collected and used for its intended purpose.
Instructions for use	Privacy Notices or Data Protection Notices	Can be compared to the GDPR's 'Privacy Notices' or 'Data Protection Notices'. These notices inform data subjects about the purpose and methods of data processing, similar to how instructions for use inform users about the intended purpose and proper use of an AI system.
Recall of an AI system	'Right to Erasure'	No direct equivalents in GDPR, as they specifically pertain to the physical or functional removal of AI systems. However, they conceptually align with GDPR's 'Right to Erasure' (also known as the right to be forgotten), which allows data subjects to have their personal data erased under certain conditions.
Withdrawal of an AI system	'Right to Erasure'	No direct equivalents in GDPR, as they specifically pertain to the physical or functional removal of AI systems. However, they conceptually align with GDPR's 'Right to Erasure' (also known as the right to be forgotten), which allows data subjects to have their personal data erased under certain conditions.
Informed consent	Consent	Closely mirrors the GDPR's concept of 'Consent'. GDPR defines consent as a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, through a statement or a clear affirmative action, signify agreement to the processing of personal data relating to them. This definition aligns with the notion of informed consent for participation in testing, emphasizing the importance of voluntariness and awareness of the testing's aspects.

Annex C – EU AI Act GDPR Equivalents: Principles

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 7: Comparison between EU AI Act and GDPR in terms of overarching principles

EU AI Act	GDPR	Comment
Human Agency and Oversight	Accountability	The EU AI Act emphasizes the importance of human oversight for high-risk AI systems, ensuring they can be effectively overseen by natural persons during their use. This aligns with the GDPR's principle of accountability, where data controllers must ensure and demonstrate compliance with data protection principles.
Technical Robustness and Safety	Integrity and Confidentiality	The EU AI Act requires high-risk AI systems to be developed based on training, validation, and testing data sets that meet quality criteria. GDPR does not directly address technical robustness but mandates the security of personal data processing through appropriate technical and organizational measures (Article 32, GDPR).
Privacy and Data Governance	Data Minimisation, Purpose Limitation and Accuracy	The EU AI Act specifies conditions for processing personal data for bias detection and correction in high-risk AI systems, including technical limitations and state-of-the-art security measures. GDPR's core focus is on the protection of personal data, with principles such as data minimization, purpose limitation, and ensuring data accuracy (Articles 5-6, GDPR).
Transparency	Lawfulness, Fairness and Transparency	The EU AI Act mandates that high-risk AI systems be designed to ensure their operation is transparent, enabling deployers to interpret the system's output and use it appropriately. GDPR emphasizes transparency in the processing of personal data, requiring clear communication to data subjects about how their data is used (Articles 12-14, GDPR).
Diversity, Non-Discrimination and Fairness	Lawfulness, Fairness and Transparency	The EU AI Act requires examination of possible biases in training, validation, and testing data sets and measures to prevent and mitigate these biases. GDPR addresses non-discrimination implicitly through the principles of fairness and accuracy in data processing and explicitly in the context of automated decision-making and profiling (Article 22, GDPR).

Table 7: Comparison between EU AI Act and GDPR in terms of overarching principles (continued)

EU AI Act	GDPR	Comment
Societal and Environmental Well-Being	No direct equivalent	While the EU AI Act does not explicitly mention environmental well-being in the provided references, it addresses societal impacts by facilitating the development of AI systems in regulatory sandboxes with safeguards to protect fundamental rights and society. GDPR does not directly address societal or environmental well-being but contributes to societal trust by enforcing strict data protection standards.
Accountability	Accountability	The EU AI Act includes provisions for record-keeping and documentation to justify the processing of special categories of personal data for bias detection and correction. GDPR establishes the principle of accountability, requiring data controllers to implement measures that ensure and demonstrate compliance with the regulation (Article 5(2), GDPR).

Annex D – EU AI Act GDPR Equivalents: Rights

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 8: Comparison between EU AI Act and GDPR in terms of rights for individuals

EU AI Act	GDPR	Comment
Right to explanation	Right of access by the data subject	The EU AI Act does not directly replicate the GDPR's right of access by the data subject. However, Article 68c provides a right to explanation for individuals affected by decisions made by high-risk AI systems, which could be seen as a form of access to information about how personal data is used in decision-making.
No direct equivalent	Right to rectification	The EU AI Act does not explicitly include a right to rectification akin to the GDPR. The focus of the AI Act is more on the systemic requirements for AI systems, including documentation, transparency, and safety measures, rather than individual rights to modify personal data.
No direct equivalent	Right to erasure ('right to be forgotten')	Similar to the right to rectification, the EU AI Act does not directly address the right to erasure. However, the Act mandates that personal data processed for bias detection and correction in high-risk AI systems must be deleted once the bias has been corrected or the data has reached the end of its retention period.
No direct equivalent	Right to restriction of processing	The EU AI Act does not provide a direct equivalent to the GDPR's right to restriction of processing. The Act's provisions are more focused on the conditions under which AI systems can process data, especially for bias detection and correction, rather than allowing individuals to limit such processing.
No direct equivalent	Right to data portability	The EU AI Act does not include a provision equivalent to the GDPR's right to data portability. The Act's scope is centered on the regulation of AI systems' development, deployment, and use, rather than on the rights of individuals to transfer their data between controllers.
No direct equivalent	Right to object	There is no direct equivalent to the GDPR's right to object in the EU AI Act. However, the Act does provide mechanisms for oversight and enforcement by national authorities, including the ability to request documentation and conduct testing of high-risk AI systems to ensure compliance with fundamental rights obligations.

Annex E – EU AI Act GDPR Equivalents: Dates

This section outlines the potential cross-overs between these two EU pieces of legislation to emphasize how making inferences can inform insights for the other (and vice-versa).

Table 8: Comparison between EU AI Act and GDPR in terms of dates

EU AI Act	GDPR	Comment
Entry into Force		
At August 2024	At May 2016	The regulation shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.
Transition Period		
August 2024 – August 2026	May 2016 – May 2018	The regulation shall apply from 24 months following its entry into force. This period allows Member States, institutions, and AI system providers and deployers to prepare for compliance. • Titles I and II, concerning prohibitions, will apply from six months following the entry into force of the regulation. • Title III Chapter 4, Title VI, Title VIIIa, and Title X, covering various regulatory aspects including penalties, will apply from twelve months following the entry into force. • Article 6(1) and corresponding obligations will apply from 36 months following the entry into force 2. Regulatory Sandboxes: By the date of general application (24 months after entry into force), at least one regulatory sandbox per Member State shall be operational, or the Member State must participate in the sandbox of another Member State.
Entry into Application		
At August 2026	At May 2018	See above.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialize in providing comprehensive and tailored solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organizations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

Acknowledgements

Corporate Partners

We are grateful to our network of corporate partners for their invaluable contributions:

Individual Partners

We are also grateful to our network of individual supporters for their invaluable contributions:

Christina Thakor-Rankin, Christina Thakor-Rankin is the CEO of Simpal.ai.

*Doug Hohulin, Business Associate (AI & Partners), Strategy and Technology Advisor on Responsible AI (Ethics, Governance, Policy, Regulation, Compliance, Safety), AI in Healthcare, and AI Operations and Workflows.

Dr Ilesh Dattani, Dr Ilesh Dattani is the CTO and Founder of Assentian - a Cyber Security and AI Lab based in the UK, USA and Ireland. Ilesh has spent the last 25 years leveraging emerging technologies like Artificial Intelligence into disruptive new innovations aimed at transforming and optimising mission and business critical systems and services across a diverse array of sectors and applications including financial services, civil aviation, construction, nuclear energy, supply-chain management and Cyber Security. He is an investor in and mentor to AI start-ups in Europe, the United States, Kenya, Singapore and Australia. Ilesh is a Certified Information Security Auditor, a Chartered Engineer and has a first degree and masters in Mathematics and a Phd in Artificial Intelligence.

Dr. Indranil Nath, Dr. Indranil is an entrepreneurial and globally exposed leader, board member, and iNED with 35 years of experience in insurance operations and technology. He has helped establish a compelling vision for information systems functions, and technical solutions, including company-wide application development in both buy and build scenarios. Indranil has consulted on the ethics of AI recommendation and independent review guidelines for Responsible AI and peer-reviewed the UN Action Plan for Sustainable Planet in the Digital Age. He has led the Operational Excellence programme and deployed digital solutions to transform business processes by automating using AI/ML capabilities. Technology Inclusion Council has awarded him the '2021 Top 100 Diverse Leaders in Tech'. He is an Honorary Senior Fellow at the School of Science & Technology, City University of London, a Chartered Engineer, a Chartered Fellow of The Chartered Institute for IT, and a Fellow of the Institute of Directors.

Kate Shcheglova-Goldfinch, Kate is on the list of Top3 UK Banker of the Year (Women in Finance Awards, 2023), TOP10 Policy makers and regulatory experts (Women UK Powerlist'23 by Innovate Finance), UN Women UK'24 Delegate developing tech diversity. Last four years Kate led the fintech and regulatory stream as an external Senior PM at EBRD, serving local central banks, creating regulatory acts and deploying regulatory sandbox legal frameworks (first global regulatory sandbox deployed under the war conditions for Ukrainian central bank, went live in March 23).

Lisa Ventura MBE, Lisa Ventura MBE is an award-winning cyber security specialist, published writer/author, and keynote speaker. She is the Founder of Cyber Security Unity, a global community organisation that is dedicated to bringing individuals and organisations together who actively work in cyber security to help combat the growing cyber threat. As a consultant Lisa also works with cyber security leadership teams to help them work together more effectively and provides cyber security awareness and culture training, and training on the benefits of hiring those who are neurodiverse. She has specialist knowledge in the human factors of cyber security, cyberpsychology, neurodiversity and AI in cyber, and is also a Co-Founder of International Imposter Syndrome Awareness Day. More information about Lisa can be found on www.lisaventura.co.uk.

Mark Smitham, Mark is passionate about helping organisations achieve their digital transformation goals by providing them with innovative and scalable solutions based on secure technology. Mark provides strategic advice for technology projects, with consideration for politics and business around the world stemming from his previous experiences of working for the British government, EU institutions, and companies from US, China, and Europe. Mark works best in diverse and multicultural environments with multidisciplinary teams of government officials, technology specialists, and legal experts. With over 19 years of experience in technology and security policy, Mark is passionate about helping organisations achieve their digital transformation goals by providing them with innovative and scalable solutions based on secure technology. He has in-depth understanding of the perspective from Brussels and EU decision-making processes in the policy areas of security and digital, with professional experience since 2014 in Brussels in EU government relations and government technology roles. Mark holds an MSc in Information Technology from the University of the West of Scotland as well as an MA in Linguistics from the University of Glasgow. He works in English, French, and Dutch, and is proficient in German and Italian.

Michael Boevink, Michael Boevink has more than 20 years management experience in the fintech and banking industry and is founder of his own investment company Boevink Group. Mr. Boevink specialises in capital raising, scaling and executing go-to-market strategies and business development growth in global markets and is engaged in companies as Raimac Financial Technology - Raimac.io - a programmable payment solution. He holds an MBA from the University of Bradford.

Neil Oschlag-Michael, Neil Oschlag-Michael works with AI, data, governance, risk and compliance. Neil writes about AI, risk, fairness and the EU AI Act and publishes the "EU AI Act Risk Master Class" newsletter on Substack. Neil holds master's degrees in data science and business administration and also has experience in IT, consultancy and healthcare sectors.

Tom Burroughes, Tom Burroughes is Group Editor of WealthBriefing, a global publication focused on covering the institutions and people looking after financial lives of high net worth and ultra-HNW clients. He has held this role since early 2008. Tom travels extensively to financial centres around the world as part of his role and has spoken on industry panels, television programmes, and taken part in podcasts. Before joining WealthBriefing, Tom was wealth management editor of The Business, a UK publication within the Telegraph Group, and prior to this, a correspondent for Reuters. He lives in London.

Vibhav Mithal, Vibhav Mithal is an Associate Partner at Anand and Anand and is practicing as an intellectual property litigator for over 8 years. Vibhav has been a part of many path breaking litigations such as the Aloys Wobben dispute (Supreme Court, 2014); Roche v. Cipla (Delhi High Court, 2015); Shree Nath v. ABD (Delhi High Court, 2015); Monsanto dispute (Supreme Court, 2019), Ferid Allani (Delhi High Court, 2019 & Intellectual Property Appellate Board, 2020) and Armasuisse (Delhi High Court, 2023). Vibhav regularly contributes to leading IPR publications such as Managing Intellectual Property magazine, Computer and Telecommunications Law Review, Asia Business Law Journal, the Intellectual Property Law Review and Patent Litigation Review and has also co-authored the India Chapter in Global Patent Litigation (3rd Edition, 2019) published by Bloomberg Law. Vibhav has also been recognized by Managing Intellectual Property as a Rising Star, 2022 and 2023.

*Doug has made significant contributions to AI & Partners over the course of its lifetime, particularly in regards to responsible AI practices, ethics, regulations, governance and policy primarily for the healthcare sector.

Important notice

Opinions in this document reflect the opinions of the authors, and are not intended to be relied upon. The authors do not accept any responsibility for any reliance placed on this document. It is important to obtain professional guidance as appropriate when seeking to deal with the matters raised in this report.

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V