



Consultation Response: Draft Cyber Security Policy Framework

OCTOBER 2025

Contents	
Background	3
Consultation engagement	3
Overall comments received on the Framework	5
Summary of responses relating to the Cyber Security Policy Framework	6
Question 1: How confident are you in Jersey’s ability to protect its digital infrastructure and respond to cyber threats?	6
Question 2: If you are unconfident, what is the reason?	6
Question3: Do you agree with the five strategic priorities in the cyber security framework?..	7
Question 4: If no, what do you regard is missing?	7
Question 5: Please rank the five strategic priorities within the cyber policy framework in order of importance to you (1= most important, 5 = least important)	8
Question 6: What support or resources would help you or your organisation improve your security practices?	9
Question 7: How do you think Jersey can better support the development of cyber skills and careers, especially among young people and underrepresented groups?	9
Question 8: What roles should the private sector, educational institutions and international partners play in strengthening Jersey’s cyber resilience?	11
Question 9: What concerns do you have about the balance between cyber security, privacy and digital innovation in Jersey?	12
Question 10: Do you have any other comments or suggestions in relation to building Jersey’s cyber security resilience that would support policy development?	13
Appendix 1: Survey responses: Respondent profile	15
Appendix 2: Addressing specific feedback on the Vision Statement and supporting Strategic Priorities	17
Appendix 3: Copy of consultation questions	19


Background

The draft [Cyber Security Policy Framework](#) builds upon the work of Jersey's first [Cyber Security Strategy](#) published in 2017. The first strategy raised awareness of the Island's cyber security vulnerabilities and the need for collective action.

Central to delivery of the first strategy was:

- the creation of a technical centre of cyber security excellence
- to support businesses and Islanders
- to share intelligence
- to defend the Island against cyber threats

As a result of the first strategy, the Jersey Cyber Security Centre (JCSC) is now operational and significant progress has been made on developing Jersey's first Cyber Security Law. This legislation will formalise the role of JCSC in co-ordinating cybersecurity intelligence and promoting good cybersecurity practice for the Island. In addition, cyber security duties will be placed on Jersey's Operators of Essential Services to improve the Island's cyber resilience.

The commitment of Government to secure trust in Jersey's digital infrastructure is reflected in the proposed Cyber Security Policy Framework:  [Draft Cyber Security Policy Framework](#)

Engagement with key stakeholders commenced in early 2025, with a series of targeted presentations to share the proposed structure of the framework and policy intent. Initial feedback was shared, which helped shape the consultation draft. A six-week public consultation was launched (22/07/2025 to 02/09/2025) to encourage wider feedback on the proposed Cyber Security Policy Framework. During this consultation period a broad range of Island stakeholders were engaged to ensure feedback was received from various of perspectives.

Feedback on the draft Cyber Security Policy Framework was specifically requested on the following areas:

- a) The proposed 5 strategic priorities of the framework and their priority for delivery
- b) Support or resources that would help improve cyber security practices of Islanders/organisations
- c) Confidence levels of Jersey's ability to respond to cyber threats and protect its digital infrastructure
- d) How to support cyber skills and careers on Island
- e) Collaboration opportunities between private sector, education institutions and international partners

Consultation engagement

Consultation feedback was collated via written feedback; orally during presentations given within the consultation period or via an on-line survey form on the Government of Jersey [Cyber Security Policy Framework consultation](#) web page.

Over the course of the consultation period, 3 briefings were held, reaching interested Islanders, businesses regulatory bodies, members of financial services and members of the Institute of Directors. These briefing reached c.88 participants. In addition, publicity of the consultation period was supported via social media advertising and pushed out to members of relevant organisations or via newsletters.

Feedback received has been taken into consideration. There were 18 complete responses captured via the online survey, and 8 email responses individually submitted via the economy@gov.je email address. Responses received were from a mix of individual and organisational responses, both on- and off-Island.

A copy of the proposed Cyber Security Policy framework and supporting consultation documentation were both publicly available via the [gov.je consultation website](#) throughout the consultation and remain publicly available.

Overall comments received on the Framework

The general feedback received was in support of the proposed cyber security policy framework in setting a vision for the Island and moving the ambition forward from the initial 2017 Cyber Security Strategy. There was support for the overarching policy goals and their strategic intent. The policy framework **sets the ambition**. To achieve the stated ambition a clear **delivery plan** needs to be developed with stated timeline, actions and identification of those responsible for delivery needs to be developed with stakeholders and strategic partners. Development of this delivery plan will be the priority in 2026 and will be incorporated into the Ministerial priorities of the next Ministerial four-year term.

It is acknowledged that since 2017 the cyber threats have significantly increased and that the narrative in the policy framework should be positioned more to discuss how we all operate within a 'cyber war zone' and the impact of rapidly advancing threat actors that act on a global scale. Policy development needs to balance driving collective action with ensuring key stakeholders and experts have the opportunity to input and shape the final outcome. This is indeed the process that will be employed to ensure a robust delivery plan that focuses on the priority areas and considers the short-, medium- and long-term impact that can be made in order to achieve the vision as outlined in this framework.

Government does play a crucial role and needs to continue to leverage cross-departmental collaboration to achieve the ambition of the framework. Digital Services sit within the Chief Minister's political portfolio, and remain responsible for the security of the Government of Jersey's digital estate and access to digital government services. All Ministers are also responsible for delivering cross-government initiatives to meet the priorities stated in the current [Ministerial Common Strategic Plan](#). This is where Island-wide concerns are addressed, such as the cost-of-living crisis, housing and retaining/attracting skilled Islanders.

Comments were raised about the use of the word 'optimising' in the vision statement. Alternatives have been considered and the vision has been updated to:

**Advancing Jersey's cyber security and cyber resilience,
enabling Islanders and businesses to prosper.**

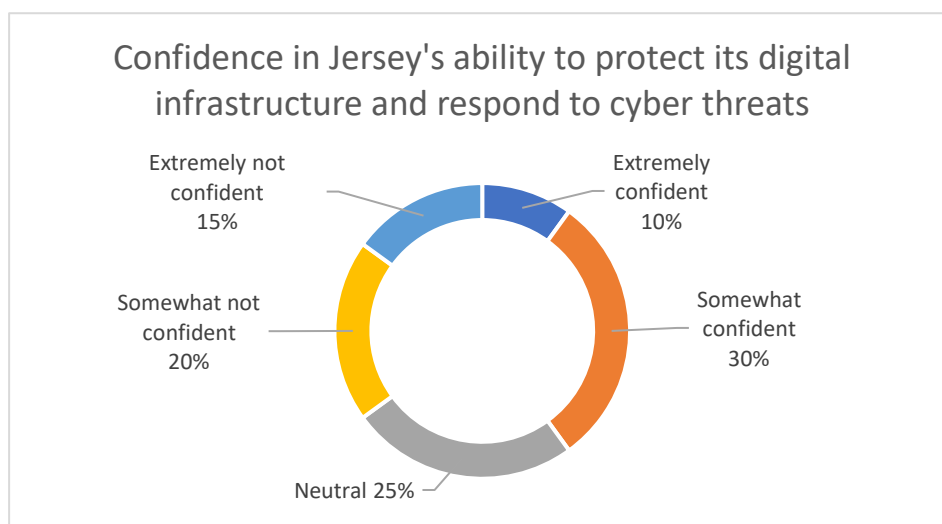
Data collected about the respondent profile can be found in Appendix 2. From this data, it can be seen that responses were mainly received from the financial service sector and technology/digital service providers with those completing the survey being aged 45+ with some cyber security expertise. Responses were also received from large organisations or bodies representing an interested group of Islanders. This indicates there is still significant work to be done for businesses and Islanders to take ownership of the security of their digital environments and become engaged with the journey to raise Jersey's cyber resilience.

A copy of the full set of questions asked in the consultation can be found in Appendix 3.

Summary of responses relating to the Cyber Security Policy Framework

Question 1: How confident are you in Jersey's ability to protect its digital infrastructure and respond to cyber threats?

Responses to this question have provided an insight into the cyber resilience perception of the Island:



Whilst 65% of those who responded to this question were neutral, somewhat confident or extremely confident over a third of respondents were not confident, and their reasoning was provided in response to question 2.

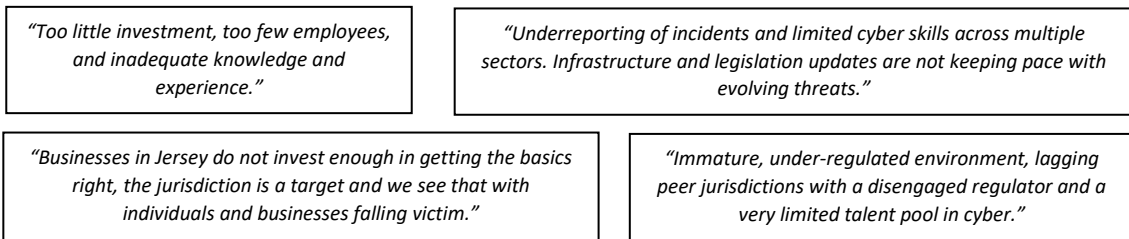
Question 2: If you are unconfident, what is the reason?

Responses to this open-ended question indicated confidence in this space needs to be strengthened by:

- Increasing investment in cyber security, both at a Government level and within local businesses to improve cyber resilience, with a focus on getting the basics right
- Recognising and utilising the pool of cyber expertise available on Island
- Supporting talent and skills development through recognised cyber skills and cyber careers pathways applicable across multiple sectors, not just within the digital entities
- Clearly establishing the role of the Jersey Cyber Security Centre (JCSC) and their relationship with the UK's National Cyber Security Centre (NCSC). Recognition of the support and expertise JCSC can draw on from more technically specialised and larger organisations, and clearly articulating how JCSC can bring this knowledge to local Jersey businesses
- Acknowledging and building on the relationships Island critical infrastructure entities already have in place with the NCSC, to increase cyber threat knowledge on Island and to supplement the local support and guidance from JCSC
- Support is needed for managing the disruptive effects of future technologies (including, but not limited to, AI developments and quantum computing)

- Improved reporting of incidents
- Ensuring continued policy and legislative alignment with Emergency Planning, Telecoms Security Framework and the developing Draft Cyber Law which need to keep pace with the changing threat landscape.

Additional comments included:



Improving confidence levels is key to future success. Whilst the future strategic ambition can and has captured the above points, they also need to be key elements of the supporting delivery plan and with appropriate outcome-based metrics.

A comparison can be drawn from the construction industry, where a holistic approach to improving health and safety has ensured not only standards have risen sharply but also the overall perception and professionalism of the sector. Learnings from this industry will be reflected on to help meet the stated ambitions of the cyber policy framework.

Question3: Do you agree with the five strategic priorities in the cyber security framework?

Of the online survey responses received, 67% responded YES and there was broad agreement of the five strategic priorities from the responses received by email. Where feedback was provided on the specific priorities of the framework, this has been summarised in Appendix 2.

Question 4: If no, what do you regard is missing?

Where negative or unsure responses were received, additional comments included:

- Closer alignment with Network and Information Systems EU legislation (NIS1 and NIS2) for CNIs: The draft Cyber Law is Jersey’s first legislative step in this respect, placing cyber security duties on Operators of Essential Services for the Island and placing clear functions and obligations on the Jersey Cyber Security Centre. Global legislative changes and implementation best practices are routinely monitored. There are expectations that legislative amends will be needed within the next Ministerial term to ensure Jersey’s security framework remains relevant.
- Develop a risk-based approach to cyber security: Such an approach evaluates the risk landscape, allowing leadership to evaluate and prioritise the most critical cyber security risks at a given time. Therefore, a key focus of this approach is on the continuous identification, monitoring and reassessment risks and the controls put in place to mitigate them. This

promotes a proactive cyber security culture and enables businesses, especially SMEs, to focus on their most significant threats and vulnerabilities. Greater emphasis of supporting a risk-based approach to cyber security will be reflected in the framework.

- Strategic priorities are too broad: Whilst the opposite may be true if elements of the framework are removed. The framework sets the ambition for the island. A delivery plan will be developed in 2026 that will be clear on the delivery priorities and will champion the focus in the short-, medium- and long terms.
- Effectiveness of the ambition undermined by overlapping reporting and the risk of regulator duplication: Whilst the total ambition of the cyber security framework does not entirely rest on timely threat information sharing, this is a critical element. It is acknowledged that the increase in reporting requirements of new security legislations for the Island can involve contacting multiple agencies, but each have their own roles and responsibilities. A key ambition of the Cyber Security Policy Framework will be to work with Jersey-based regulatory bodies, Jersey Financial Services Commission, Jersey Office of the Information Commissioner and Jersey Competition and Regulatory Authority to help reduce the duplication of information reported, and therefore make the reporting of cyber incidents easier for all.

Question 5: Please rank the five strategic priorities within the cyber policy framework in order of importance to you (1= most important, 5 = least important)

The consultation responses indicated that *‘Strengthening the cyber security within businesses, organisations and for Islanders’* was most important to them. With *‘Growing cyber security skills and capabilities’* and *‘Continual development of an Island-wide resilient digital ecosystem’* a close second and third priority:



The order of the five strategic priorities within the Cyber Security Policy Framework will remain in the current order. The importance and challenge of growing cyber security skills and capabilities is not underestimated and this will require strong political engagement across ministerial portfolios in order to deliver to expectations.

The importance of *‘Responding to the rise in cybercrime’* should not be overlooked, for a few respondents this was listed as a second priority.

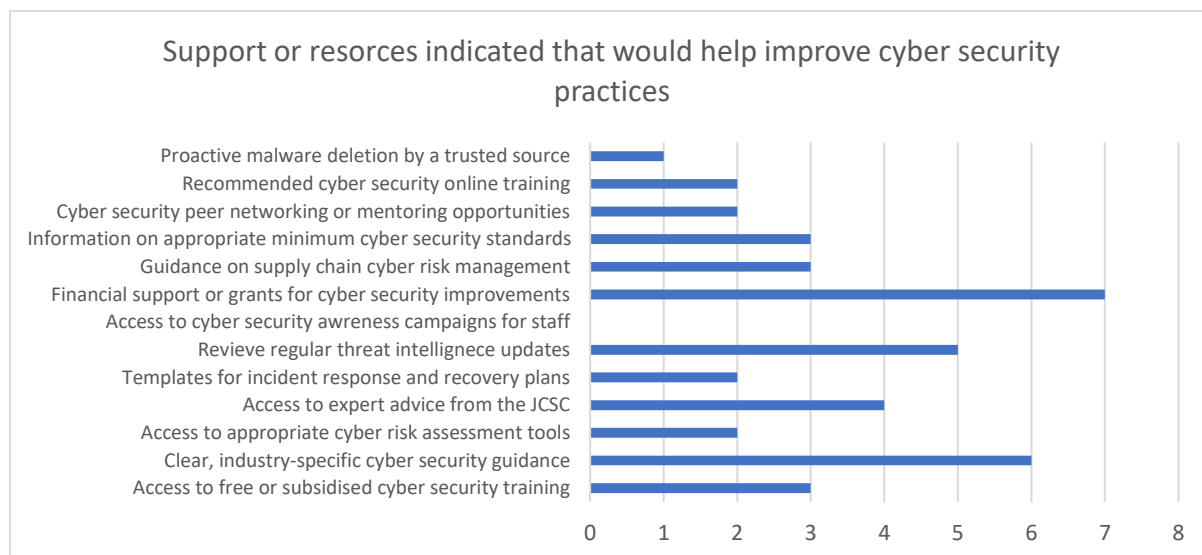
These views will help shape delivery priorities and focus in the short-, medium- and long-term.

Question 6: What support or resources would help you or your organisation improve your security practices?

Beyond providing financial support or grants for cyber security improvement, access to clear, industry-specific cyber security guidance was highlighted as a key resource that would help improve security practices, alongside receiving regular threat intelligence updates.

Business should feel they can turn to the Island’s technical advisory body on cyber security, the Jersey Cyber Security Centre, for relevant expert guidance across a number of cyber security topics, and their role in this space needs to be firmly established and maintained moving forward. As a small team, JCSC work closely with the UK’s National Cyber Security Centre (NCSC) and are able to draw on the vast body of information, guidance and tools they create, for implementation in Jersey. Therefore, as highlighted in a number of responses, these resources do not need to be developed from scratch and should become easily and readily available in Jersey. This role of the JCSC will be further highlighted within the Cyber Security Policy Framework.

Receiving regular threat intelligence updates was also seen to help improve cyber security practices. Once received, action needs to be taken by the receiving body, if threat intelligence is to be of any benefit. This is where the JCSC can support the local business community and develop closer working relationships with the digital suppliers on- and off- Island, operators of the Island’s essential services and larger expertise bodies, such as the UK’s NCSC.



Question 7: How do you think Jersey can better support the development of cyber skills and careers, especially among young people and underrepresented groups?

This was an open-ended question to identify areas of interest and concern to address this with respect to the stated ambition in Strategic Priority 3, growing cyber security skills and capabilities.

A number of responses suggested developing partnerships with local businesses to expand Trident work experience opportunities, local delivery of the NCSC's CyberFirst programme, summer placements, internships, practical work experience opportunities and apprenticeships. Links could be built with secondary schools as well as with Highlands - giving all students a chance to meet relevant role models, understand the different career pathways into the industry and to get relevant work experience. Such partnerships could help deliver the above mentioned extra-curricular activities and work will continue with digital service providers on Island as to how they can help be part of the solution moving forward. The ambition within the policy framework will remain the same.

The GoJ supported Digital Apprenticeship with Exeter University is already available for local businesses to support the skills development of either new recruits or current staff. Very few businesses in the industry have taken up the opportunity, indicating continued marketing and promotion of the scheme is needed.

The NCSC's CyberFirst scheme was developed to create opportunities for students to consider a career in future-focused tech areas including cyber security, AI, quantum computing, software and data. This scheme has only been run in a few secondary schools on-Island and competes with other extra-curricular pressures on teaching staff and school budgets.

Based on the success of the NCSC's CyberFirst programme in the UK, the Prime Minister [announced](#) at the London Tech Week on 8 June 2025, a commitment to invest £187 million embedding AI and technology throughout education and launching a TechFirst programme to be delivered via the Department of Science Innovation and Technology (DSIT). The importance of investing and developing skills in our young Islanders is key and work in this policy space will continue in close collaboration with CYPES.

Career development of professionals was also highlighted as needing to be encouraged, where a recognised industry body ensures cyber careers are championed and attainment of relevant professional standards are encouraged and provide networking opportunities. The Channel Islands Information Security Forum could be well placed to help develop and promote career development opportunities and this has been reflected in the framework.

Within Government, Digital Services have committed to develop an ***"I.T. Skills Academy Programme - a five-year initiative to grow in-house technical talent, reduce reliance on contractors and sustain a skilled IT workforce"*** as part of the Government's [IT Strategy](#). Digital Services are currently in the process of determining how the programme should be established and delivered to raise digital skills within Government.

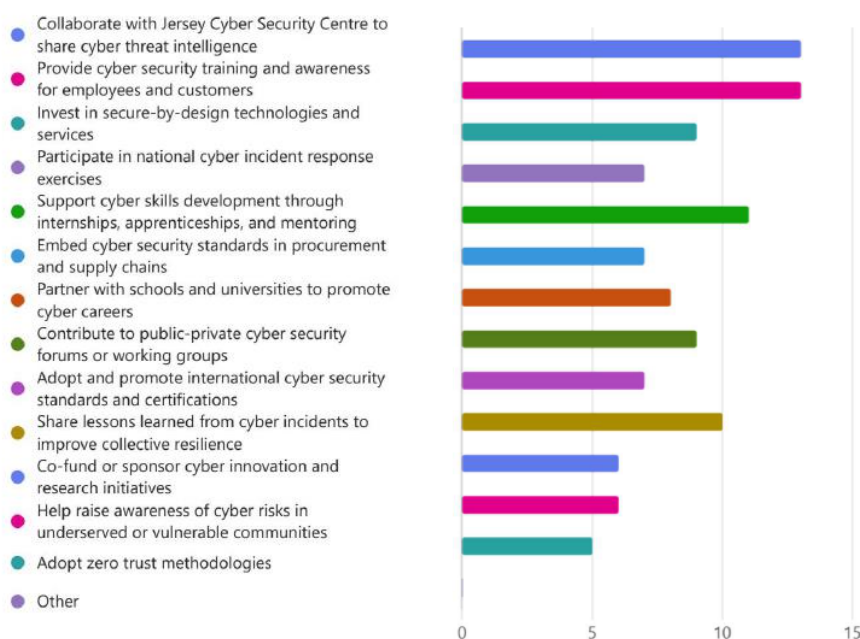
A few interesting thoughts were shared on cyber skills funding, where ideas for conditional grants to fund tertiary education or for subsidies for companies to take on apprentices were put forward.

Snapshot of further comments can be found below:

<i>"Promote and enhance the existing GoJ Digital Apprentice scheme and partnership with the University of Exeter."</i>	<i>"Partnerships with schools for training and with professional bodies to include relevant training in professional qualifications."</i>
<i>"Launch a visible 'Cyber Pathways programme' that begins in primary school...."</i>	<i>"... Fund paid 1 – 4 week summer micro-internships across local security teams so teenagers experience real-world impact...."</i>
<i>"Partnerships with schools for training and with professional bodies to include relevant training in professional qualifications."</i>	<i>"Investment in developing skills and careers in the digital sector... Cyber Security should be a key factor, but they often form an intrinsic part of digital skills these days...."</i>
<i>"Establish a centralised industry body to advocate for cyber careers and standards."</i>	<i>"The local opportunities for learning and developing cyber security skills tend to focus on foundational concepts, such as basic cyber hygiene, awareness of common threats, and networking/IT knowledge."</i>
<i>"Free/subsidised taster training."</i>	
<i>"Government backed service offerings, that are certified and cost effective to check websites / applications and even things like site pen testing."</i>	

Question 8: What roles should the private sector, educational institutions and international partners play in strengthening Jersey's cyber resilience?

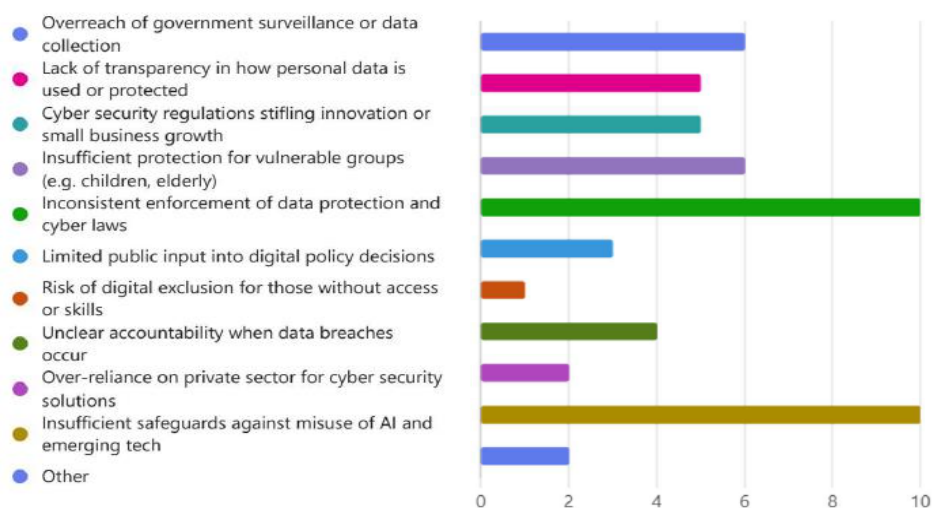
From the responses provided, there is a recognition that whilst Government does play a key role in championing the need to raise the cyber resilience of Jersey, the wider ecosystem does need to lean in, as everyone plays a vital part. Managing expectations around collaboration and shared responsibility will play a key role in the success and delivery of the cyber security policy framework. Even if local businesses championed only two of the following activities in 2026 and 2027, a difference would be made:



Government can lead by example, with the need for Digital Services and Jersey Cyber Security Centre to work closely together for example to share threat intelligence and for active participation in national cyber response exercises and share lessons learned. Digital Services are also looking at developing specific training routes to develop digital skills within their team, as captured in their summary IT Strategy for Government: [Government of Jersey I.T. Strategy Executive Summary](#). Digital Services are developing the programme and delivery mechanisms and further details are not yet available.

Question 9: What concerns do you have about the balance between cyber security, privacy and digital innovation in Jersey?

Feedback was sought to understand the current perspectives of Jersey’s legislative and regulatory frameworks to help address current concerns and to shape Jersey’s longer-term ambition in this area in the future.



Concerns continue to be raised about the difference in reporting times for significant cyber incidents and personal data breaches. Education and guidance will be provided about the different roles of the Jersey Cyber Security Centre, a centre of expertise, and the role of Jersey based regulators. Future consideration to simplify reporting requirements to reduce duplication will also be considered as part of the delivery plan.

Globally, jurisdictions are looking at policy levers as well as legislative and regulatory frameworks for governance of new and emerging technologies. These legal frameworks are to underpin national AI strategies or ethics policy and AI governance legislation. As per data protection, the EU has taken a centralised approach with the formal adoption of the AI Act in 2024, compared with the US’s decentralised approach. In all cases, the overlap of data privacy and data security are highlighted and the challenges around enforcement should not be underestimated.

The overlap of data privacy and data security will be further emphasised in the Cyber Security Policy Framework as Jersey looks to address these challenges and concerns of the security of emerging technology.

Question 10: Do you have any other comments or suggestions in relation to building Jersey's cyber security resilience that would support policy development?

Responses to this open-ended question has provided a wide range of comments, which can be summarised as follows. Where more general responses were received, comments have been captured in Appendix 2.

Incorporate the concept of improving cyber security hardness through jointly reducing the attack surface and vulnerabilities. This should be driven by attackers and their evolving threat capability globally and externally. As an approach to mitigate risk this can be incorporated into the policy framework. and the concept can be extended to mitigate cyber risks as reliance on emerging technology e.g. AI increases. These points will be emphasised in the updated cyber security policy framework.

Whilst resilience has not been specifically defined in the framework, [The National Institute of Standards and Technology](#) in the US, (NIST) has defined resilience as *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption*. Resilience includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents. The UK's [National Cyber Security Centre](#) (NCSC) considers the term 'cyber resilience' as referring to *"an organisation's ability to maintain the correct operation of its essential functions even in the presence of adverse cyber events."* The NCSC's definition will be explicitly defined within the final Cyber Security Policy Framework, where "organisation" can refer to an individual as well. Adopting this definition of cyber resilience supports a risk based approach to cyber security, where risks occurring as a result of a cyber incident are identified and appropriately mitigated.

Elevate the importance of supply chain security and increase commitment to drive security in this area. This is incorporated within the framework and will be reviewed to further elevate its significance.

Security of emerging technologies. The cyber security policy framework will be revised to reflect the need to address both the security of emerging technologies and where such technologies can be used for criminal activities. One specific reference was made to help highlight the importance of guarding against generative AI-voice cloning, which is driving CEO fraud and is linked to the rise in identity theft.

The Government's approach to ransomware attacks should be clarified: There is significant movement in this space by larger jurisdictions and best practice will continue to be reviewed to formulate an appropriate and proportionate policy position. Whilst there is not currently a specific requirement to report crime related to ransomware, there are requirements in the Proceeds of Crime (Jersey) Law 1999, the Money Laundering Order 2008 and the Terrorism (Jersey) Law 2002 to report

money laundering and terrorism financing to the Financial Intelligence Unit. Further policy development in this space is expected in the next Ministerial term.

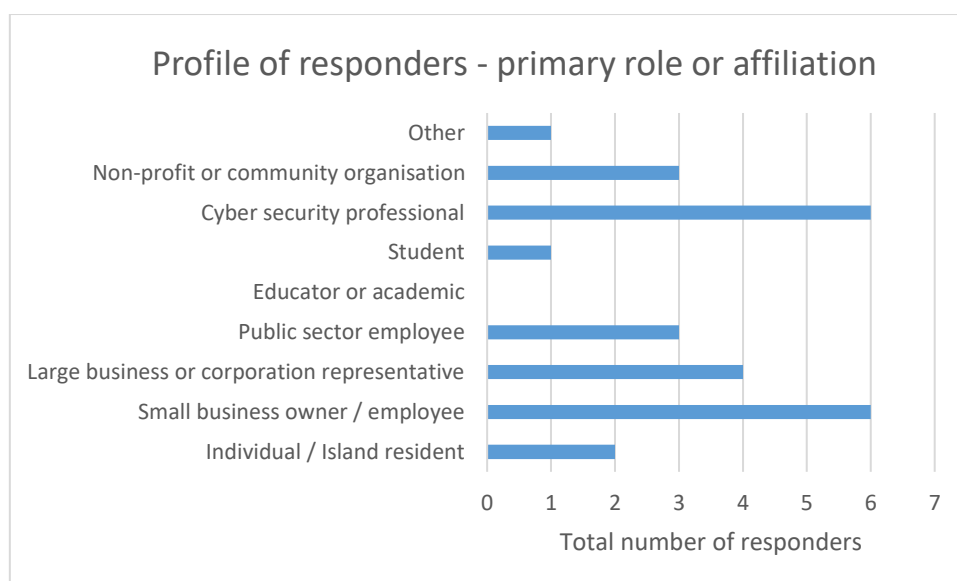
Recognising the convergence of cyber and financial crime: This will accelerate as emerging technologies further enable illicit opportunities to be taken. The Financial Action Taskforce and Financial Intelligence Unit already work closely with Jersey Cyber Security Centre and wider stakeholders to understand how cybercrime and cyber security vulnerabilities are exploited and how this links to financial crime and illicit finance. In turn leading to updated policy positions and relevant supporting legislation and regulations. Narrative will be strengthened in the policy framework.

Alignment with organisations that have deep cyber expertise: It is recognised that Jersey based consultancies have skills and expertise that can be drawn on, as do larger and more mature organisations (e.g UK's NCSC) where Jersey has existing relationships. All provide a wealth of cyber security expertise that can be utilised to help raise cyber resilience, provide career path opportunities and help bring local cyber support to smaller businesses. Emphasis should be placed on a collaborative approach and ensuring the limited resources in Jersey do not duplicate efforts.

Appendix 1: Survey responses: Respondent profile

The first five consultation questions were to gain an understanding of the respondent profile, which can be summarised as follows. The full set of consultation questions can be found in Appendix 3.

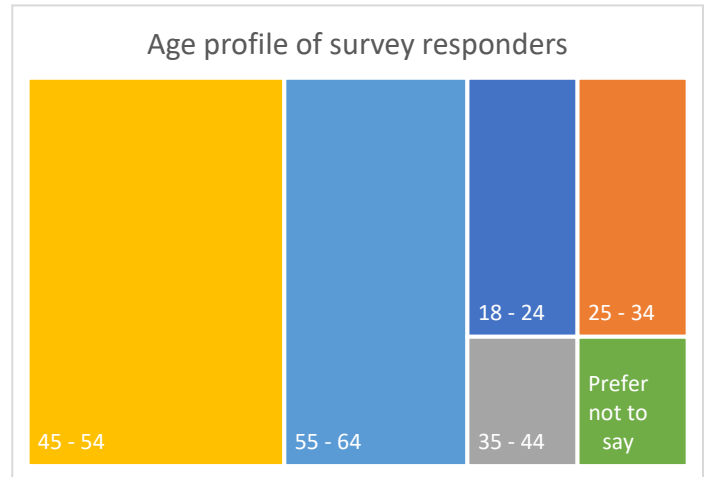
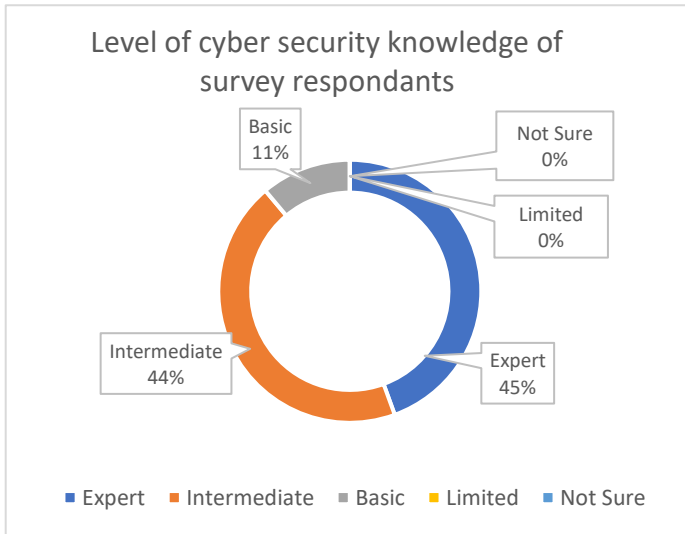
The declared primary role or affiliation of responders highlights the role of the small business in Jersey's economy and the interest of cyber policy professionals in the framework. Whilst no responses were specifically received from educators/academics, CYPES have been involved in the development of the cyber security policy framework.



Responses to the online survey were received predominately from the financial service and the technology/digital service sectors, where cyber security is vital for the operating reputation of the company:

Business sector	% of responders, where declared
Financial Services	35%
Technology or digital services	42%
Education	0%
Healthcare	0%
Government / public administration	8%
Retail or hospitality	0%
Legal or professional services	8%
Not currently employed	0%
Other	8%

With survey feedback being predominately provided by those with a professional 'expert' or 'intermediate' level of cyber security knowledge and falling within the 45 – 64 age range:



Based on the responder profile, policy engagement with under-represented business sectors will be a future priority to share the ambition of the framework and ensure they are actively engaged in building their own cyber resilience. Ambition and delivery, against the proposed ambition, will still need to address the concerns and needs of our Island experts and provide the necessary reassurance that building the Island’s future cyber resilience should not fall solely to cyber/technical experts or the financial services industry. Both sectors do have the resources and/or skills to help drive an Island-wide culture change and therefore need to remain engaged to help champion the need to increase cyber resilience.

Two responses were received from those not living or working on Jersey, providing an insight into the growing importance of Jersey’s wider cyber security resilience and reputation. Cyber security does not respect geographical boundaries and can directly impact economic wellbeing, a key element of the sustainable wellbeing of Islanders.

Not captured in the above data was the profile of those that attended the presentations. This included members of the Jersey Institute of Directors, covering a range of business sectors and the drop-in session hosted interested Islanders, members of the cyber insurance industry and Island regulatory bodies and representatives of some larger technical organisations.

Appendix 2: Addressing specific feedback on the Vision Statement and supporting Strategic Priorities

Strategic priority 1: Strengthening cyber security within businesses organisations and for Islanders

Recommendation to work in partnership with Jersey Institute of Directors to deepen understanding of cyber at a corporate level. This will be emphasised in the framework in the relevant priorities.

Recommendation that capability is developed through collaboration and not duplication. It was highlighted that the current technical capability of JCSC is limited and that Jersey should be able to pull on established relationships with mature and larger organisations in the UK, such as the NCSC. JCSC has not been established to replicate the NCSC, rather enable a strong working partnership, ensuring Jersey can benefit from their extensive expertise, training materials and skills development opportunities and promote them in a Jersey context. This will be emphasised in the updated framework.

Strategic priority 2: Continual development of an Island-wide resilient digital ecosystem

Recommend to increase the visibility of the Financial Intelligence Unit and development of closer working relationships with JCSC. This will be addressed in the updated framework.

Ambition to change culture and create an Island-wide ecosystem is challenging. This is recognised and will take time. Therefore, remains an ambition of the proposed framework.

Recommendation to review Strategic Priorities 1 and 2 and potential overlap of ambition for some policy areas. This will be reviewed in the updated framework.

Strategic priority 3: Growing cyber security skills and capabilities

Recommendation to ensure training pathways cover both the development of foundational awareness as well as advancing technical skills. This will be addressed in the updated framework.

Recommendation to seek new and alternative ways to expand skill development both in schools and professionally for example access to safe simulation platforms where learners can practice technical skills without risk to live systems. This will be addressed in the updated framework.

Strategic priority 4: Responding to the rise in cybercrime

Recommended increase the visibility and educational outreach and the role of the Financial Intelligence Unit. This will be addressed in the updated framework where appropriate.

Recommended to ensure the narrative is inclusive of crimes against businesses and emerging cyber threats and JCSC's role in this space, as well as focusing under crimes against the individual. This will be addressed in the updated framework where appropriate.

Strategic priority 5: Building a thriving cyber industry

Recommended to increase the emphasis to addressing the Island's challenges around retaining Islander's, declining birth rates, cost of living, housing etc. which all have an impact on attracting and retraining talent into the cyber security industry. These are all key priorities and concerns that are addressed the current [Ministerial Common Strategic Plan](#). Therefore, will not be addressed specifically in the cyber security policy framework.

Recommended to improve the policy stance and guidance from Government and regulatory bodies to support the adoption of new technologies, e.g. FinTech. This will be emphasised in the updated framework.

Recommended to consider the incentives to entice both existing or new providers to establish a business on Jersey. This will be considered alongside the [Trade, Investment and Growth Framework](#).

Concerns raised that focusing on building a thriving cyber industry detracts from the priority message that strong cyber security is an economic enabler which can build and retain trust across the economy. As highlighted the survey responses, strategic priority 5 was not a top priority but will remain part of the Minister for Sustainable Economic Development's ambition for the Island, and supports delivery of the Digital Economy Framework.

Appendix 3: Copy of consultation questions

Respondent Profile Questions

1. What is your primary role or affiliation? (*Select one that best describes you.*)

- Individual/Island resident
- Small business owner or employee
- Large business or corporate representative
- Public sector employee
- Educator or academic
- Student
- Cyber security professional
- Non-profit or community organisation
- Other (please specify): _____

2. What sector do you primarily work in (if applicable)? (*Optional – select one*)

- Financial services
- Technology or digital services
- Education
- Healthcare
- Government/public administration
- Retail or hospitality
- Legal or professional services
- Not currently employed
- Other (please specify): _____

3. How would you describe your level of cyber security knowledge? (*Select one*)

- Expert – I work in cyber security or a related field
- Intermediate – I have some training or responsibility for cyber security
- Basic – I understand the risks and take basic precautions
- Limited – I rely on others for cyber security
- Not sure

• **4. What is your age group?**

- Under 18
- 18–24
- 25–34
- 35–44
- 45–54
- 55–64
- 65+
- Prefer not to say

5. Do you live or work in Jersey? (*Optional – select one*)

- Yes – I live in Jersey
 - Yes – I work in Jersey
 - Yes – I live and work in Jersey
 - No – I am responding from outside Jersey
-

Survey questions relating to the Cyber Security Policy Framework

1. How confident are you in Jersey's ability to protect its digital infrastructure and respond to cyber threats? (Scale Options – select one):

- Very confident
- Somewhat confident
- Neutral
- Somewhat unconfident
- Not confident at all

2. If you are unconfident, what is the reason?

[Open ended question, response limited to 500 characters]:

3. Do you agree with the five strategic priorities in the cyber security framework? (Options – select one):

- Yes
- No
- Unsure

4. If no, what do you regard is missing?

[Open ended question, response limited to 500 characters]:

5. Please rank the five strategic priorities within the cyber policy framework in order of importance to you (1 = most important, 5 = least important)?

(Please rank in order of importance):

- Strengthening cyber security within businesses, organisations, and for Islanders: *Ensuring everyone understands cyber threats, adopts protective measures, and can recover from attacks.*
- Continual development of an Island-wide resilient digital ecosystem: *Building strong partnerships, legislation, and infrastructure to support long-term cyber resilience.*
- Growing cyber security skills and capabilities: *Developing a skilled workforce and career pathways to support the Island's cyber future.*
- Responding to the rise in cybercrime: *Enhancing law enforcement capabilities and public awareness to combat digital crime.*
- Building a thriving cyber industry: *Fostering innovation, investment, and economic growth in the local cyber sector.*

6. What support or resources would help you or your organisation improve your cyber security practices?

Suggested Options (Please tick all that apply or suggest others):

- Access to free or subsidised cyber security training
- Clear, industry-specific cyber security guidance
- Access to appropriate cyber risk assessment tools (e.g. Jersey Cyber Shield)
- Access to expert advice from the Jersey Cyber Security Centre (JCSC)
- Templates for incident response and recovery plans
- Receive regular threat intelligence updates
- Access to cyber security awareness campaigns for staff
- Financial support or grants for cyber security improvements
- Guidance on supply chain cyber risk management
- Information on appropriate minimum cyber security standards
- Cyber security peer networking or mentoring opportunities

- Recommended cyber security online training
- Proactive malware deletion by a trusted source
- Other (please specify, *max 300 characters*): _

7. How do you think Jersey can better support the development of cyber skills and careers, especially among young people and underrepresented groups?

[Open ended question, *response limited to 1000 characters*]:

8. What roles should the private sector, educational institutions, and international partners play in strengthening Jersey’s cyber resilience?

Suggested Options (*Please select those you believe are most important.*)

- Collaborate with Jersey Cyber Security Centre to share cyber threat intelligence
- Provide cyber security training and awareness for employees and customers
- Invest in secure-by-design technologies and services
- Participate in national cyber incident response exercises
- Support cyber skills development through internships, apprenticeships, and mentoring
- Embed cyber security standards in procurement and supply chains
- Partner with schools and universities to promote cyber careers
- Contribute to public-private cyber security forums or working groups
- Adopt and promote international cyber security standards and certifications
- Share lessons learned from cyber incidents to improve collective resilience
- Co-fund or sponsor cyber innovation and research initiatives
- Help raise awareness of cyber risks in underserved or vulnerable communities
- Adopt zero trust methodologies
- Other (please specify, *max 300 characters*): _____

9. What concerns do you have about the balance between cyber security, privacy, and digital innovation in Jersey?

Suggested Concerns (*Please select the top 3 concerns that matter most to you.*):

- Overreach of government surveillance or data collection
- Lack of transparency in how personal data is used or protected
- Cyber security regulations stifling innovation or small business growth
- Insufficient protection for vulnerable groups (e.g. children, elderly)
- Inconsistent enforcement of data protection and cyber laws
- Limited public input into digital policy decisions
- Risk of digital exclusion for those without access or skills
- Unclear accountability when data breaches occur
- Over-reliance on private sector for cyber security solutions
- Insufficient safeguards against misuse of AI and emerging tech
- Other (please specify): _

10. Do you have any other comments or suggestions in relation to building Jersey’s cyber security resilience that would support policy development?

[Open ended question, *response limited to 1000 characters*]:
