10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

techUK Response

Home Office: Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting

08/04/2025

Contact: Annie Collings, Programme Manager, Cyber Resilience: annie.collings@techuk.org

Executive Summary

techUK welcomes and shares the government's ambition to ensure the UK is better protected against ransomware. techUK also appreciates that this Consultation has been issued to complement work already taking place across government and industry to increase the cyber resilience of organisations, the Public Sector and Critical National Infrastructure (CNI) whilst protecting digital technology users. The cyber threat landscape and particularly the ransomware ecosystem is evolving to become increasingly complex and professionalised, and it targets all parts of the UK and global economies. The UK is in the position to lead and showcase its strengths within cyber resilience in a variety of ways on the global stage, however, there is still much more to be done to protect organisations at scale. It is, therefore, crucial that the government uses all appropriate and available solutions to prioritise and tackle ransomware.

techUK and its members recognise the serious threat ransomware poses to organisations and the wider economy; however, any new guidance or frameworks must be carefully designed to avoid further burdening the victims of ransomware attacks and to prevent any unintended consequences, particularly for small to medium-sized enterprises (SMEs) and individuals. We feel strongly that victims need support not punishment. This support should be available quickly and come in the form of intelligent, practical advice for the appropriate times where paying the ransom is the judicious thing to do. At the same time, these measures should provide government with the necessary intelligence to respond effectively to the threat of ransomware.

We believe that a broader approach is required to mitigate the risk of ransomware. A blanket ban on ransomware payments could be problematic – for example, banning payments could inadvertently push ransomware transactions underground, reduce visibility into cyber criminal activities and/or shift attacks to other sectors outside UK CNI and the Public Sector, such as Manufacturing which contributes a significant amount to the UK economy, or further down the supply chain. Indeed, it is recognised that cyber criminals will simply pivot and adapt when certain avenues are cut off to them. Instead, techUK members would encourage the government to further explore the prevention mechanisms that target ransomware at its source and improve the UK's cyber resilience.

While a ransomware payment prevention regime could reduce the number of ransomware payments being made to criminals, techUK and its members also find this proposal problematic. We tend to disagree with an outright economy wide payment prevention regime, as this universal approach fails to account for the varying capabilities and resources of different organisations and would be very costly to enforce and maintain – intelligent triage here is essential. It would align more closely with the government's ongoing cyber ambitions to spend money and efforts on building up the UK's national cyber resilience. Applying a blanket payment prevention requirement to all organisations could create serious operational risks, particularly where critical data or operations are at stake.

While improved reporting is certainly beneficial, techUK members believe that a blanket approach could create disproportionate challenges for particular groups that may lack the resources or expertise to comply. The UK's current voluntary ransomware incident reporting regime should continue to be used with a more structured approach which ensures organisations see the value in reporting, rather than perceiving it as an additional regulatory burden. To encourage compliance, the government should share anonymised threat intelligence from reports, providing businesses with actionable insights on the emerging ransomware tactics used by nation states and cyber criminals. A threshold-based approach would help balance reporting obligations while capturing critical incidents. Furthermore, many techUK members have also suggested that a single portal, or one-stop shop, for reporting incidents should be adopted to make compliance less burdensome.

Throughout the response, techUK and its members highlight the importance of aligning this consultation's scope with the definition of CNI in the Cyber Security and Resilience Bill, currently being developed by the Department for Science, Innovation and Technology (DSIT). The consultation's scope should also align with terminology used in other relevant government policies such as the Position, Navigation and Timing (PNT) Strategy. There should also be consistency in the terminology used, including terms such as 'Arms-Length Bodies' and 'ransomware'. It is important to note that the last few years have been particularly busy in the policy space, for both the cyber security sector and the wider technology industry in the UK. Even larger digital companies with their own dedicated public affairs and policy teams have faced capacity challenges with the volume of regulatory reporting requirements that have been introduced through new legislation and Codes of Practice. With this in mind, the government must ensure there is alignment with existing regulatory frameworks to avoid duplication and excessive administrative burdens – particularly for SMEs and sectors that already have significant reporting requirements in place – for example, financial services organisations.

techUK has encouraged members to submit individual responses where they can showcase evidence gathered by their own organisations that can better inform some of the topics at hand.

The UK's public–private cyber partnership remains strong and, on behalf of the cyber security and broader technology industry, techUK is committed to helping government address the ever-evolving threat landscape and close the gap between the threat and our exposure to it, and the defences that are in place to protect us. techUK is, therefore, eager to facilitate continued engagement between the Home Office and industry, on government's plans to protect the UK from ransomware attacks, as well as efforts to build a more harmonised approach to security resilience.

Answers to consultation questions

Survey Questions

Section 2: Proposal 1 - Targeted ban on ransomware payments

A ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure (that are regulated, or that have competent authorities)**.**

Scope outline
The questions below are largely directed at those CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, but we also welcome responses from others who have an interest in these sectors.

Q10. To what extent do you agree, or disagree, that HMG should implement a targeted ban on ransomware payments for CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government.
1 □ Strongly agree.
2 □ Tend to agree.
3 □ Neither agree nor disagree.
4 □ Tend to disagree.
5 □ Strongly disagree.
99 □ Don't know.
Please provide any further explanation for your response [free text]:

techUK welcomes and shares the government's ambition to address the threat that ransomware attacks pose to the UK – in particular, our critical national infrastructure (CNI) – especially as these attacks become more sophisticated and prolific as criminals get better at using, for example, AI. techUK members, however, doubt that a payment ban will stop attackers from deploying ransomware or indeed undertaking other forms of cyber extortion and they are concerned about the unintended consequences of an outright ban on ransomware payments for CNI owners and operators and the public sector. For example, any exemption for 'threat to life' incidents could encourage cyber criminals to target infrastructure that while not included in the exemption could still lead to a 'threat to life'. This would push ransomware payments to an 'underground' market which could, in turn, lead to less government visibility of payments. Another one of these consequences could be attackers simply deflecting to other non-CNI/public-sector targets such as the Manufacturing sector, which are worth a considerable amount to UK PLC, as well as having the potential to impact on supply chains in related sectors. Indeed, we can expect criminals to do what they do best and adapt, or pivot – moving the problem elsewhere.

Initiatives carried out by law enforcement and the National Cyber Security Centre (NCSC) have been shown to disrupt the ability of criminal groups, with figures showing ransomware payments fell dramatically in the latter half of 2024.[1] It is important that their work to disrupt and deter ransomware attacks is applauded.

[1] The Guardian (2025) Global ransomware payments plunge by a third amid crackdown

Any ban on ransomware payments presents a number of challenges, not least of which would be how government would implement, administer and enforce it. Criminal organisations often work outside of the UK's jurisdiction, and, without international alignment, such a ban could be ineffective. A ban on payments also removes a mechanism which some organisations will use to recover from attacks, when they feel they have no other means. Indeed, the consequences of prolonged downtime could be severe, particularly on the UK's health and emergency services, where an inability to operate could lead to the loss of life. As a result, and contrary to the Government's ambition, the ban on ransomware payments may actually increase the attractiveness of attacks on CNI, albeit where the attacker aims to cause maximum disruption to CNI sectors rather than monetary gain. techUK understands that the Home Office has undertaken some scenario planning with regards to its proposal, however, members have flagged that much more of this may be required to understand the true impact. Indeed, previous pieces of legislation have undergone extensive scenario planning due to the complexity of the threat – with members citing the four years of scenario planning for the Investigatory Powers Act as one example of this.

It has been highlighted that, given there is the potential for an outright ban to be ineffective in terms of acting as a preventative measure, it would be undertaking a significant risk to trial it through the UK's CNI – that is, testing its efficacy on assets that are essential to the functioning of our society.

A further consideration should be that, if the ransom is not paid by an organisation in compliance with the ban, and then personally identifiable information (PII) is leaked, who will assume responsibility/liability for that leak?

techUK members are also concerned that if the government decides to make the payment of ransomware an offence, this will only cause further impact on the victim rather than the criminals responsible for the attack or, in other words, further punishing the victim. Victims need support not punishment. Members see this as a rule which would create further missed opportunities with identifying and charging criminals.

In the event that government decide to proceed with this proposal, further work must be carried out to refine the definition of which CNI sectors fall in scope. There should be alignment between this consultation and the Cyber Security and Resilience Bill, as well as the definition used in other government policy such as the PNT Strategy. Furthermore, the government should consider adopting tiers for adoption based on relevant revenue thresholds. This would take a proportionate approach to adoption– for example, the Communications CNI sector is a very wide and diverse sector with large multinationals and much smaller SMEs. The question of extraterritorial scope must also be reflected upon further. To this point, it would be useful for the government to understand whether the proposed payment ban in the UK may impact on CNI in other countries who may be paralysed by a ransomware attack that cannot be resolved through payment of the ransom. techUK members have proposed that only the UK operations of a company should fall in scope as this makes it easier to define, enforce and avoids conflicts with similar requirements in other countries, for example, Australia.

A ban, if extended into the supply-chain for CNI operators (as incident reporting requirements are, for example under Cybersecurity Maturity Model Certification (CMMC) for the Department of Defense (DoD) supply chain in the US), may also act as a deterrent to innovative organisations considering the "dual use" potential of their technology to the CNI of the UK

Some techUK members who operate in the digital assets sector have highlighted that when a payment has been made, those funds and their proceeds can be traced along the relevant blockchain and recovered privately or via law enforcement. In some cases, the payment of ransoms (using the addresses which receive the payment) can also assist in identifying the threat actor via data attribution, which in certain circumstances, unmask and prosecute those parties. This is a key part of intelligence building and taking down broader criminal networks that ransomware attackers are generally part of. One member suggested creating a solution where payments are still an option that either a company chooses, or the government decides is a strategic option for disruption of a particular criminal actor or network. This option, however, would need to be managed closely in a number of ways. This could be that payments are made through seized reserves which are held by the UK government, a threshold is agreed so that payments need go over a certain amount or that a third party analytics company be deployed to tag and follow the assets deployed as part of a payment.

Separately, one member highlighted that some organisations may not have the technical ability to pay via crypto currency. By joining the payment activity to law enforcement and intelligence, there is the possibility to follow the money, rather than trying to do that post transaction some time later, and the victim will feel supported, not persecuted. It's also important that this service must be responsive and not, for example, a month-long decision matrix. One techUK member highlighted the role email service providers should play in providing ransomware protection through blocking known malware.

While techUK members are concerned about the unintended consequences of an outright ban on ransomware payments for CNI operators, they are in favour of government supporting organisations, businesses and individuals to become more cyber resilient. Members suggested, therefore, that should this proposal be introduced, a more nuanced approach is taken, focused on building cyber resilience, and that government engages further with industry to refine its approach, to ensure that any measures taken are both effective and proportionate.

Q11. How effective do you think this proposed measure will be in reducing the amount of money flowing to ransomware criminals, and thus reducing their income?
1 □ Effective
2 □ Somewhat effective
3 □ Neither effective nor ineffective
4 [✓ □ Somewhat ineffective]
5 □ Ineffective
99 □ Don't know.

Q12. How effective do you think banning CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, from making a payment will be in deterring cyber criminals from attacking them?
1 □ Effective
2 □ Somewhat effective
3 □ Neither effective nor ineffective
[✓ 4 □ Somewhat ineffective]
5 □ Ineffective
99 □ Don't know.

Q13. What measures do you think would aid compliance with the proposed ban? *Select all that apply.*
1 □ Additional guidance to support compliance with the ban.
2 □ Tailored support to manage the response and impact following an attack.
98 □ Other, please specify *[free text]*
96 □ None [free text]
99 □ Don't know.

To support compliance with a proposed ban on ransomware payments, techUK members believe the government would need to develop a number of different support mechanisms tailored towards organisations operating in different sectors and of different sizes.

The government should provide clear and explicit guidance which has a detailed overview of the steps organisations should take in the event of a ransomware attack and should proactively engage in supporting CNI sectors to respond and recover if required. It is in the government's interest to do so. This is particularly true if nation state actors choose to follow this path of attack. This guidance should include alternative recovery options, if payments are no longer allowed. A sector-specific framework should be developed to ensure there is clarity on the compliance requirements and practical steps for reporting incidents, without losing the ability to easily correlate the potential threat of incidents crossing over between sectors.

One techUK member suggested developing sector-specific guidance, this should be provided by regulators, translating the legal terminology into what the introduction of a ban would mean for their respective sectors, including practical examples.

If these proposals are to become legislation, then government must provide a clear understanding of the definitions of CNI and the public sector. By straying from the definition used across other parts of government, in particular the Cyber Security & Resilience Bill, the legislation threatens to become an additional piece of red tape which impacts on its operability. The government should define what constitutes an 'essential supplier' and the remit for this role. Members also asked for further clarification on the government's definition of an ALB often these types of organisations will run their own IT systems through Managed Service Providers (MSP). If a ban is to be introduced, would the risk lie with the private sector suppliers of this IT?

One techUK member also highlighted that the current proposals include a very narrow definition of ransomware. Currently, other forms of cyber extortion such as a distributed denial-of-service (DDoS) are not covered. This could end up creating a displacement of energies or result in cyber attackers changing their tactics to continue inflicting harm. Another techUK member suggested reframing the definition of ransomware to specifically software or to explicitly exclude ransom attacks that are related to DDoS. The government should also ensure that the definition of payments does not include payments to ethical hackers which are not classified as malicious.

techUK members agreed that businesses tend to pay ransoms if they cannot guarantee that they can recover the targeted data in a timely manner. The government should invest in the national cyber response teams that can rapidly assist affected CNI operators and organisations who need to recover from an incident. Delays in the process could lead to further harm to the victim.

On this point, cyber insurance will and can help businesses in their ability to react and recover to incidents, however, the fact that organisations are encouraged to hold cyber insurance, sometimes gives the business a false sense of security that they are covered from any type or scale of attack. It is critical that anyone in an organisation who is responsible for buying and processing cyber insurance into the business, fully understands what the policy covers and what it does not. If ransomware payments are banned, the government must clarify the role of cyber insurance and how affected organisations can recover financially without relying on insurance-driven ransom payments.

Insurance companies must also understand their own liability and be clear as to whether their customers are under-insured or have the necessary level of measures in place so that if an incident occurs, they are able to react and recover in the most risk-free way. Should this proposal be introduced, there should also be clarity on the impact on insurance premiums to ensure SMEs are not disproportionately affected. One techUK member suggested that, given the number of insurance companies offering cyber security cover, compared to the number of organisations within the UK's CNI, that insurance companies be obligated to report any claims and details of their interactions with attackers.

Government must be able to demonstrate the success of banning ransomware payments in order to incentivise organisations to comply.

Q14. What measures do you think are appropriate for non-compliance with the proposed ban?
Select all that apply.
1 □ Criminal penalties for non-compliance
2 □ Civil penalties for non-compliance
98 □ Other, please specify *[free text]*
96 □ None [free text]
99 □ Don't know.

Building on the themes raised in the answers to Questions 10 and 13, techUK members strongly disagree with this proposal. However, if government does proceed then non-compliance should be scaled and proportionate based on organisational size and the severity of the breach to prevent a disproportionate impact on SMEs.

techUK members are strongly not in favour of criminalising victims of a ransomware attack, finding any such initiative counterproductive to the government's own resilience agenda. Penalising organisations for paying a ransom would unfairly shift the burden onto those already impacted by cyber-crime, rather than addressing the root cause. Even those companies that have mature information security policies cannot guarantee 100% attack resistance – particularly when they are targeted by nation states. Building on this, the impact of striking off individuals on Boards, who make decisions on paying ransoms, could overlook the complexities of the often-extreme circumstances which surround these decision-making moments. For multi-national organisations, these Boards often sit outside of the jurisdiction of UK law, therefore, a more nuanced approach is needed to avoid undermining intelligence gathering by security companies and law enforcement that track ransomware payments to criminal networks. This further emphasises the need to refine and clarify the scope of entities subject to the proposed obligations.

When looking at implementing any measures for non-compliance, the government must also define at what point in the supply chain organisations fall under the scope of the proposed legislation. Many

CNI operators rely on private sector IT suppliers and without clear guidance on whether third-party providers would be subject to compliance requirements, businesses risk inadvertently being non-compliant to the proposed ban. This guidance should be produced by the relevant regulatory authority which is most appropriate to each sector.

One techUK member highlighted the importance of insurance companies having a clear baseline for compliance. This will improve overall maturity of security, and the cost of successful attacks will increase alongside the probability of being targeted decreasing.

Q15. If you represent a CNI organisation or public sector body, would your organisation need additional guidance to support compliance with a ban on ransomware payments?
1 □ Yes
2 □ No
99 □ Don't know.
[✓ 100 □ Not applicable]
If yes, what support would you need? [free text]:

Once again building on the themes raised in the response to Q10 and 13, techUK members believe clear and explicit guidance is needed to support organisations who have fallen victim to a ransomware incident. Indeed, if the government moves forward with the proposal to ban payments, they should continue to provide guidance which has a detailed overview of the steps organisations should take in the event of a ransomware attack. This guidance should include alternative recovery options, if payments are no longer allowed.

The National Cyber Security Centre (NCSC) has positioned itself as the organisation that businesses can go to for guidance and support if they fall victim to an attack. However, some techUK members note that currently, there is often a diversion between the NCSC's discouragement of paying a ransom and external legal advice which may in some circumstances advise the victim/organisations to pay. The threat is perceived as much more fluid now and guidance for both the public sector and private sector and the approach should be much more joined-up.

To support compliance, the government should make it easier to respond to an attack. Currently, when a system is attacked, one of the things that creates blurred lines in the response is the time it takes to recover critical systems. This is due to three things:

1. Size of the data – and the extended time it takes to restore.
2. Lack of regular testing of an organisation's restoration process – knowledge of any vulnerabilities of the hardware/software/cloud-based solutions that are being used are a key element of resilience against any form of cyber-attack.
3. Lack of a thoroughly tested incident response plan.

It is important for businesses specifically to ensure that they can meet the recovery time that they set, and what is required for them to recover efficiently. techUK members agreed that businesses tend to pay ransoms if they cannot guarantee that they can recover the data targeted in a timely manner.

Members highlighted that for public sector bodies and extending out to CNI organisations that are subject to regulation like the upcoming Cyber Resilience and Security Bill, the NCSC can signpost to existing services, in particular Cyber Incident Response and Assured Cyber Security Consultancy

(ACSC), for tailored application of guidance to the organisation and support them in understanding and maturing their cyber resilience.

techUK members once again reiterate the need for clear definitions of CNI, the public sector, ALBs and 'essential suppliers'. By straying from the definition used across other parts of government in particular the Cyber Security & Resilience Bill, the legislation threatens to become a further piece of red tape which impacts on its operability. The government should also define what constitutes an 'essential supplier' and the remit for this role. Again, being clear on the scope of the entities subject to the proposed obligations is vital here when proposed sanctions include criminal offences.

Q16. Should organisations within CNI and public sector supply chains be included in the proposed ban?

1 ☐ Yes, please provide details *[free text]*
2 ☐ No, please provide details *[free text]*
99 ☐ Don't know.

As already highlighted in the response to Q10, organisations that operate within the UK's CNI and public sector supply chains play a critical role in maintaining our national infrastructure. While there is a clear need to strengthen cyber security resilience, techUK members highlighted several complexities that could have unintended consequences if you bring supply chain organisations under the scope of the ban.

Ransomware attacks are often carried out by international crime groups, who operate beyond the reach of UK law. While they may target UK CNI and public sector, the organisations who operate within these supply chains could be large multi-nationals whose headquarters are based outside of the UK. The decision for paying a ransom is often at a Board level, these Boards may be based outside of the UK and therefore also fall outside of UK law. Government should also offer clarification on the extent to which supply chains will be impacted by the ban. For large multi-nationals whose supply chains operate internationally there will again need to be clear guidance on which parts of the supply chain fall under scope of the legislation.

Further, it would be helpful if the government clarified how it intends to include suppliers to CNI and public sector in this proposal. For example, is it the case that the suppliers will be directly in scope of the ban and therefore subject to the same enforcement/penalty system? Or would it be the expectation that CNI and public sector will need to contractually agree that their suppliers comply with the ban? If the latter, should all suppliers be in scope, or only a subset? Any contractual work with suppliers takes time and therefore sufficient lead in time to amend contracts should be built in if the latter option is pursued.

techUK members are also concerned that a targeted ban may not deter cyber criminals but rather redirect their efforts to vulnerable sectors who do not fall into scope of the ban. Criminals adapt their strategies, and a CNI and public sector specific ban could incentivise them to target other industries, such as manufacturing or retail. Criminals could also change their tactics, shifting to a blackmail-based attack or threaten to deploy malware unless a ransom is paid. These evolving tactics, make it difficult for a blanket ban to truly decrease the threat of ransomware on the UK's economy. By excluding certain parts of the supply chain from the ban, the government could unintentionally expose vulnerabilities. A cyber-attack on a supplier, such as a transport company that delivers to water treatment facilities, could have consequences on CNI operations and the government should consider whether a broader, sector agnostic approach is required to cover all crime types where a ransom is associated with a cyber-attack or threat of a cyber-attack. As mentioned previously, there is a risk that a ban on ransomware payments may actually increase the attractiveness of attacks on CNI, albeit where the attacker aims to cause maximum disruption to CNI sectors rather than monetary gain. The government should also consider whether the regulator would need to inform parts of the supply chain that they fall under scope of the legislation, due to a lack of clarity on where the line is drawn on which parts of the supply chain are included.

Ultimately, while there is an argument for including supply chain organisations within the scope of the ban if government proceeds, the decision must be accompanied by clear legal definitions, robust enforcement mechanisms, and appropriate support structures to mitigate unintended consequences. The government must also consider how this aligns with existing legislation, to avoid regulatory inconsistencies that could create compliance challenges for affected organisations.

Q17. Do you think there should be any exceptions to the proposed ban?
[✓ 1 □ Yes]
2 □ No
99 □ Don't know.
If yes, please provide *further explanation for your response? [free text]:*

This question was answered in Q10 & 16.

Q18. Do you think there is a case for widening the ban on ransomware payments further, or even imposing a complete ban economy-wide (all organisations and individuals)?
1 □ Yes widen the ban.
2 □ Yes impose a complete ban economy-wide.
[✓ 3 □ No]
99 □ Don't know.
If yes widen the ban, please provide further explanation for your response [free text]:

Section 3: Proposal 2 – A new ransomware payment prevention regime

A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.

Please find the relevant information on Proposal 2: A ransomware payment prevention regime in paragraphs 50-62 and Figure 3 in this consultation document.

Q19. To what extent do you agree, or disagree, that the Home Office should implement the following (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by	**Threshold-based payment prevention regime, for certain organisations and individuals**	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but**	**Threshold-based payment prevention regime for certain organisations not covered by the**

	the ban set out in Proposal 1.	**not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Strongly Agree				
2 Tend to agree				
3 Neither agree nor disagree				X
4 Tend to disagree	X	X	X	
5 Strongly Disagree				
99 Don't know				

Please provide any further explanation for your responses [free text] (optional):

techUK and its members recognise the government's aim to reduce the financial incentives for ransomware attacks, however, the unintended consequences of a broad payment prevention regime and the disproportionate impact it may have on certain organisations, including SMEs is concerning.

Some techUK members tend to agree with a threshold-based payment prevention regime for certain organisations not covered by Proposal 1. A targeted approach that considers organisational size, sector and the financial impact of an attack would help balance the UK's security objectives with operational resilience. SMEs often lack the financial resilience and security maturity of larger organisations, an outright payment prevention regime could put them at significant risk of business closure. One techUK member also raised concerns around the government's power to 'block' payments. They noted that this would be a complex initiative to implement given the range of stakeholders the government would need to develop relationships with.

techUK and members tend to disagree with an outright economic-wide payment prevention regime, as this universal approach fails to account for the varying capabilities and resources of different organisations and would be very costly to enforce and maintain. It would align more closely with the government's ongoing cyber ambitions to spend money and efforts on building up the UK's national cyber resilience. Applying a blanket payment prevention requirement to all organisations could create serious operational risks, particularly where critical data or operations are at stake. One techUK member highlighted that the government already operates a UK financial sanctions guide, which includes guidance on ransomware, to stop organisations paying certain actors. As this is already in place, it may be more effective to enhance this list rather than implement a whole new framework.

If government does decide to introduce this proposal, a more proportionate approach would be to combine a threshold-based reporting model with robust support structures for affected organisations. This includes the development of clear guidance for alternative recovery options, streamlined reporting processes and enhancing government's incident response capabilities.

techUK and its members note that a nuanced, sector specific approach would be more effective in improving cyber resilience than a blanket prevention regime that does not account for real-world operational challenges.

Q20. How effective do you think the following will be in reducing ransomware payments? (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	**Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Effective				
2 Somewhat effective				X
3 Neither effective nor ineffective				
4 Somewhat Ineffective		X	X	
5 Ineffective	X			
6 Don't know				

Q21. How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors? (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	**Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Effective				
2 Somewhat effective				
3 Neither effective nor ineffective				
4 Somewhat Ineffective		X		X
5 Ineffective	X		X	
6 Don't know				

<u>Q22. If we introduced a threshold-based payment prevention regime, what would be the best way to determine the threshold for inclusion? *Please select all that apply.*</u>

1 □ Organisation's annual turnover in the UK
2 □ Organisation's number of employees in the UK
3 □ The sector the organisation is operating in.
4 □ Amount of ransom demanded.
98 □ Other, please specify *[free text]*

While techUK and its members tend to disagree with Proposal 2, if government does proceed it should consider taking a scaled and proportionate approach based on organisational size to prevent a disproportionate impact on SMEs.

99 □ Don’t know.

Q23. What measures do you think would aid compliance with a payment prevention regime? *Please select all that apply.*
1 □ Additional guidance to support compliance.
2 □ Support to manage the response and impact following an attack.
98 □ Other, please specify *[free text]*
96 □ None [free text]
99 □ Don’t know.

techUK and its members noted that guidance which has been produced by organisations such as the NCSC has been well received by industry. However, additional guidance and support following an incident would better incentivise compliance. The government must take a balanced approach that combines clear guidance and robust support mechanisms with meaningful incentives for organisations. The government should be clear on the effectiveness of a payment prevention regime to ensure ransomware payments are not driven underground or they risk reducing opportunities to track and disrupt criminals.

One measure which could aid compliance is clear and consistent communication from government. Given the number of pieces of legislation which organisations must understand not just in the UK but internationally, government should be clear about why reporting requirements are being introduced and how the information provided by industry will be used. One member highlighted the history of access to incident reporting information voluntarily shared by industry within Cybersecurity Information Sharing Partnership (CiSP) not being retained by NCSC when it decommissioned the partnership in 2024, the perceived lack of consistency across regulatory authorities with different reporting mechanisms and requirements and the lack of adoption of industry standards for that information. By being clear on the rationale behind the payment prevention regime, government can create a sense of purpose that encourages compliance rather than making organisations feel burdened by regulation.

Robust support will be critical for any payment reporting regime and this will require properly skilled resource to guide the victims of ransomware attacks throughout the process in a timely manner. Members also raised that there may be a need for Service Level Agreements (SLAs) between the victim and law enforcement to ensure that there are no unnecessary delays in the process that would themselves have a negative impact on the victim. Clear decision timelines and a professional service will be required. When considering the impact of this service provision, it should be noted that spikes in ransomware activity could impact the delivery of services outlined in the SLAs.

Currently, there is a lack of consistent and coordinated information collated by a central source within government on cyber incidents generally and ransomware in particular. A change to this would give both the UK cyber security sector and the public, a full picture of the current threat landscape (including, specifically on ransomware). As government policies are introduced to tackle ransomware, techUK members questioned whether a newly formed organisation could assess whether policies are working. Its role could be to invest time in pulling together different streams of data sources from ransomware attacks, inputting this into a central source of data to assess what the threat landscape looks like. Information can then be communicated externally to the private sector and the cyber security industry to offer solutions.

One techUK member highlighted the importance of understanding what motivates organisations to comply. Some businesses may respond to financial incentives, such as grants or reduced insurance premiums for those who meet best practice. While others may be driven by reputational concerns, which could mean organisations who comply are publicly recognised.

Government should also consider the practical support it can offer to organisations, particularly SMEs who may lack the experience to understand the steps they need to take when navigating ransomware threats. There should also be a distinction made between ransomware reporting and cyber incident reporting, if an SME needs to report an incident, they may not consider whether it is a ransomware attack or a general cyber incident. This should be clarified and should be considered when looking at the practical implementation of the measures, with a goal to minimise the number of times that an SME needs to report the same incident

A well supported organisation is more likely to comply with a payment prevention regime than one that feels isolated or overwhelmed by a new piece of legislation. By combining clear communication, meaningful incentives, adequate resourcing, behavioural insights, and practical support, the government can foster a compliance culture that encourages organisations to act in the collective interest rather than fearing punishment for being a victim of cybercrime.

Q24. Do you think these compliance measures need to be tailored to different organisations and individuals?
1 ☐ [✓ Yes]
2 ☐ No
If yes, please provide more details on how you think they should be tailored to different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

If government does decide to introduce this proposal, techUK and its members believe it is important that compliance measures are tailored to different organisations and individuals to ensure that they are effective and proportionate. Any sweeping compliance measures risk creating undue burdens, particularly on SMEs, which can lack the financial, technical and human resources to navigate complex regulatory landscapes.

Whilst a ransomware payment prevention regime is well intended, it could place smaller businesses in an impossible position where compliance means losing their businesses. One techUK member highlighted that SMEs may perceive the regulatory risk of compliance as too high, whether due to potential fines or excessive reporting requirements, they may be disincentivised from innovating or even from participating in sectors covered by the legislation.

To address the disparities, SMEs should be supported through tailored guidance, financial support and technical assistance to help them to comply with the measures. Acknowledging that smaller businesses often feel personally attached to their operations, there should also be a clear support system in place to help them recover from attacks without needing to resort to paying ransoms.

Ultimately, compliance measures should balance security with economic sustainability. Without tailored approaches, there is a risk that well-intended policies could inadvertently penalise smaller organisations, discourage transparency, and even stifle innovation in industries that rely on emerging businesses.

Q25. What measures do you think are appropriate for managing non-compliance with a payment prevention regime? *Please select all that apply.*
1 □ Criminal penalties for non-compliance
2 □ Civil penalties for non-compliance
[✓ 98 □ Other, please specify *[free text]*]
96 □ None *[free text]*
99 □ Don't know.

As highlighted in response to Q10 and 15, techUK members are concerned that introducing criminal penalties would be counterproductive to the government's own resilience agenda. If the government penalise an organisation for being non-compliant with a payment prevention regime, they would unfairly shift the burden onto those already impacted by cyber-crime. The government should consider how they are incentivising organisations. This could be through the development of a one-stop shop for reporting an incident (including ransomware) and their intention to make a ransomware payment and receiving support on the next steps.

Q26. Do you think these non-compliance measures need to be tailored to different organisations and individuals?
[✓ 1 □ Yes]
2 □ No
If yes, please provide more details on how you think they should be tailored to different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

This question was answered in Q24. One techUK member highlighted that the term 'Board' should be considered as an option. This is because the Board is the main vehicle in which businesses make large monetary decisions, including investment into cyber security.

Q27. For those reporting on behalf of an organisation, who do you think should be legally responsible for compliance with the regime?
[✓ 1 □ The organisation]
2 □ Named individual.
3 □ Both
4 □ Not applicable. I am responding as an individual
99 □ Don't know.

Q28. For those reporting on behalf of an organisation, do you think any measures for managing non-compliance with the regime should be the same for both the organisation and a named individual responsible for a ransomware payment?
1 □ Same
[✓ 2 □ Different]
3 □ Not applicable. I am responding as an individual
99 □ Don't know.
Please provide any additional comments [free text]

This question was answered in Q10 and 15.

Section 4: Proposal 3 – A ransomware incident reporting regime

A ransomware incident reporting regime. That could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

Q29. To what extent do you agree, or disagree, that the Home Office should implement the following (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident reporting regime.	Economy-wide mandatory reporting for all organisations and individuals.	Threshold-based mandatory reporting, for certain organisations and individuals. *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	Mandatory reporting for all organisations excluding individuals. *This would exclude individuals from the regime but apply it to all organisations.*	Threshold-based mandatory reporting, for certain organisations excluding individuals. *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Strongly Agree	X				
2 Tend to agree					
3 Neither agree nor disagree			X		X
4 Tend to disagree		X		X	
5 Strongly Disagree					
99 Don't know					

Please provide any further explanation for your responses [free text] (optional):

techUK and its members support the continuation of the existing voluntary ransomware incident reporting regime, while also recognising the need for a more structured approach to reporting, using the opportunity to unify existing inconsistent and disparate reporting mechanisms. Indeed, techUK members have highlighted as an example of an effective (and clearly signposted) single reporting mechanism government's Tell Us Once service. Indeed, we believe that any mandatory reporting framework must be carefully designed to avoid undue burdens on organisations and individuals while still providing government with the necessary intelligence to respond effectively to ransomware threats and to share that to the benefit of industry and the wider economy.

To ensure organisations see the value in reporting rather than just the regulatory burden, the government should share anonymised threat intelligence gathered from reports, allowing businesses to benefit from insights on emerging ransomware tactics. Organisations that report in good faith should receive legal safe harbour protections to encourage transparency without fear of reputational or regulatory repercussions.

The NCSC has done a great job at positioning themselves as an organisation that businesses can speak to if they fall victim to an attack. However, there is evidence that among industry, victims – particularly members of the public – struggle to get the help and support they require post-attack. What happens next must be made clear and support must be available.

techUK and its members tend to disagree with the implementation of an economy-wide mandatory reporting requirement for all organisation and individuals. While improved reporting is essential, a blanket requirement could create disproportionate challenges, particularly for individuals and SMEs that may lack the resources or expertise to comply effectively. Mandatory reporting for individuals could place unnecessary pressure on victims, especially those who are not cyber security experts. In sectors like healthcare or finance, techUK members noted that the general population could suffer mentally damaging effects of embarrassment or loss of dedication to work if cyber hygiene and security is not held to a higher level of concern.

techUK and its members believe that a separate reporting requirement for ransomware is not a route that should be taken. It would be more appropriate to look at cybercrime reporting across the whole sector. Any approach that government takes need to avoid creating regulatory burdens on SMEs and individuals who may struggle to navigate complex reporting obligations. The government must ensure that any threshold-based model aligns with existing reporting frameworks, such as GDPR, UK Telecoms Security Act, NIS Regulations (both existing UK and EU NIS2) and that certifications such as ISO 27001 or CE/CE+ are taken into consideration, to avoid duplication or undue burden.

techUK and its members believe any reporting framework should prioritise the support of victims, ensure clarity in reporting expectations and align with existing regulations. The government must also clearly outline how reported data will be used and what support will be offered to organisations.

Q30. How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK? (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident	**Economy-wide mandatory reporting for all organisations**	**Threshold-based mandatory reporting, for certain**	**Mandatory reporting for all organisations**	**Threshold-based mandatory reporting, for certain**

	reporting regime.	**and individuals.**	**organisations and individuals.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**organisations excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Strongly Agree					
2 Tend to agree					
3 Neither agree nor disagree	X	X	X	X	X
4 Tend to disagree					
5 Strongly Disagree					
99 Don't know					

Q31. How effective do you think the following would be in increasing the Government's ability to tackle and respond to the ransomware threat to the UK? (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident reporting regime.	**Economy-wide mandatory reporting for all organisations and individuals.**	**Threshold-based mandatory reporting, for certain organisations and individuals.** ***For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.***	**Mandatory reporting for all organisations and individuals.**	**Threshold-based mandatory reporting, for certain organisations excluding individuals.** ***This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.***
1 Effective					
2 Somewhat effective	X				X
3 Neither effective nor ineffective					
4 Somewhat ineffective		X	X	X	
5 Ineffective					
99 Don’t know					

Q32. If we introduced a mandatory reporting regime for victims within a certain threshold, what would be the best way to determine the threshold for inclusion? ***Please select all that apply*.**
1 □ Organisation’s annual turnover in the UK
2 □ Organisation’s number of employees in the UK
3 □ The sector organisation is operating in.
4 □ Amount of ransom demanded.
98 □ Other, please specify *[free text]*
99 □ Don’t know.

techUK and its members believe that the threshold for a mandatory reporting regime should be based on a combination of issues, including the organisational impact, an organisation’s sector and the severity of the attack. A nuanced approach should be taken to ensure the reporting requirements capture the most critical incidents without overburdening businesses with the number of regulatory requirements they must report, this would be most costly to SMEs.

To ensure that compliance is manageable, the government should create a centralised reporting platform, a one-stop shop, that simplifies the process for businesses. The platform should allow organisations to report once, with the information disseminated to relevant authorities, such as the Information Commissioner's Office (ICO) and sector regulators/competent authorities under NISD. It should also provide immediate guidance to organisations on the next steps they should take, including recovery options, access to expert resources and legal obligations. The government should consider the user experience and create an intelligent triage process to ensure people are given support and all the information they need to take the appropriate next steps for their business and security.

The effectiveness of a reporting regime will depend on the government's capacity to handle incoming reports. If mandatory reporting is introduced, the authorised government body must have the resources to respond to reports in real time. techUK members suggest that the government assess the impact of the activity undertaken by the NCSC to provide support to organisations.

One techUK member suggested that the incident threshold should be based on the type of data the entity in question holds or controls and the possible operational impact of the unavailability of that data. While a ransomware incident is technically just another type of cyber security incident, it is considered by the government as a separate incident, as it is seen as particularly pernicious given it encrypts data. Therefore, it's the value and criticality of the data that should determine and drive the thresholds of a possible incident reporting obligation.

A mandatory reporting regime should strike a balance between capturing critical incidents and avoiding unnecessary burdens on businesses, particularly SMEs. Thresholds should be based on business impact, sectoral importance, and data sensitivity rather than financial limits. The government must ensure that reporting mechanisms are streamlined, response capabilities are well resourced, and incentives are in place to encourage compliance. If implemented correctly, a well-structured reporting regime could improve national resilience against ransomware while fostering greater cooperation between industry and government.

Q33. What measures do you think would aid compliance with a mandatory reporting regime? *Please select all that apply*.
1 ☐ Additional guidance to support compliance.
2 ☐ Support to manage the response and impact following an attack.
98 ☐ Other, please specify *[free text]*
96 ☐ None [free text]
99 ☐ Don't know.

techUK and its members believe reporting obligations should align with the Cyber Security & Resilience Bill proposals and the GDPR reporting timelines. They should also be phased based on the timeline of the incident response process. An initial notification should be required within 72 hours for significant incidents, with minimal detail required at this stage, while full incident reports should be submitted within a longer timeframe, such as one month, once organisations have completed their internal investigations. Regulators must also ensure that reporting deadlines account for weekends and non-working hours, as small incident response teams may not be able to meet 24-hour deadlines, hence why 72 hours is more reasonable.

There needs to be a sustained effort to de-shame incident reporting. Government uses guidance through regulatory levers to encourage organisations to report incidents but as a result, organisations are punished – through media shaming – rather than incentivised to report incidents. techUK members suggested that perhaps a cultural shift is needed here with softer measures applied. As evidenced through the Government Cyber Security Strategy 2022, government plays the role of an exemplar in this case.

techUK members agreed that despite the guidance that is published by the NCSC and the wider government, organisations tend to still do the least possible in terms of reporting ransomware and cyber-attacks, by abiding by the minimum regulatory requirements. Organisations might be hesitant to share information on cyber incidents if they do not see tangible benefits in return. Government should ensure that those who comply with reporting obligations receive actionable insights on the incidents they report. These insights should include practical steps which look to improve the UK's cyber resilience. If organisations feel they gain valuable intelligence from compliance, they will be more likely to engage with the process rather than seeking ways to circumvent the rules.

There should be harmonisation between this piece of policy work and the Cyber Resilience and Security (CSR) Bill. It is vital that there is clarity in scope between the two documents and clarity on the reporting zones, which either overlap or do not include certain principles. International examples, like the Network and Information Systems 2 Directive, EU Artificial Intelligence Act and Digital Operational Resilience Act have demonstrated that a difference in reporting requirements across multiple pieces of legislation can create grey areas, which leads to underreporting. techUK members believe the government must ensure that this proposal does not inadvertently hinder efforts or create missed opportunities. For example, public sector is included in the scope of this policy proposal, but government departments are not falling into scope of the CSR Bill. Similarly, telecoms operators have their own reporting regime under the UK Telecoms Security Act 2021 and Communications Act 2003 which also covers ransomware incidents.[2] For entities that provide multiple services including CNI, across multiple security-related legislative regimes, the burden of reporting is large and complex. Building reporting systems to meet these disparate requirements is difficult and may ultimately slow down reporting to relevant authorities due to the need for manual checking against the reporting criteria for each framework. This creates confusion and ultimately leads to missed reporting opportunities.

One techUK member suggested that the government should consider whether anonymous reporting for organisations would be beneficial. This could help organisations to get over the fear of reporting and associated enforcement from regulators.

To avoid significant over reporting, that is likely to be burdensome to both NIS regulated entities and the regulators themselves, the government should clearly define what is meant by 'capable of' and what systems are captured in this. This should consider and set thresholds for:

- the level of access obtained i.e. privilege
- the volume of access obtained i.e. % of estate
- business criticality of the systems effected

[2] Ofcom (2003) https://www.ofcom.org.uk/siteassets/resources/documents/phones-telecoms-and-internet/information-for-industry/network-and-information-systems-regulations/general-statement-of-policy-under-section-105y-of-the-communications-act-2003.pdf?v=329224

- sensitivity of information as it relates to business processes or digital infrastructure and the impact of the misuse

Government should use this opportunity to streamline and unify the reporting mechanisms for cyber security incidents including ransomware attacks. Currently, there is a lack of consistent and coordinated information collated by a central source within government or partners on cyber security incidents including ransomware. A change to this would give the UK cyber security sector and the public, a full picture of the current threat landscape on ransomware. Empowering organisations to report ransomware incidents and receive guidance on next steps in a centralised location. This should include access to incident response services, technical recovery assistance and cyber security best practices to help organisations recover without resorting to paying the ransom. This type of guidance would be particularly useful to SMEs who often lack the resources or money to respond to attacks.

The effect of increasing the amount of mandatory incident reporting is to reduce the voluntary information sharing, especially where each regulatory body has different reporting regimes. Harmonising those and using technology to enable those affected by an incident to share once, in a standards-compliant way (e.g. STIX/MITRE Att&ck), and automatically securely syndicating only the relevant information to each notification point will increase the likelihood of people reporting, the quality of the information and the ability to process and act on it in an automated fashion. techUK members noted that currently too much responsibility for handling reports in the UK is left to the Competent Authorities who have a limited or no understanding of cyber incidents, and diverse reporting mechanisms and requirements, resulting in very low levels of reporting, and an inability to benefit from the data.

To further support compliance, government should properly resource the body responsible for analysing and acting on the data shared by organisations. Increased incident reporting should lead to meaningful action, such as improved national threat intelligence and more effective disruption of cyber criminals. Transparency in this process is critical, publishing anonymised data can help organisations to benchmark their security controls and take proactive steps to mitigate threats. Government should also look to simplify the reporting process, in regards to the number of bodies organisations are expected to report to. Currently, organisations are reporting to NCSC, ICO for GDPR, Action Fraud and Law Enforcement. It is important that government consider how they can automate this process and make it as simple as possible for businesses. This would increase compliance and improve support businesses when they have been a victim of an attack.

The government should be clear about what they intend to do with the data they already have, before implementing new reporting requirements. It's important that the reporting data which is provided is used to protect organisations, the economy and public services to continually learn lessons and improve security processes. At the moment, the landscape is incredibly fragmented with organisations reporting to NCSC, ICO, Action Fraud and Law Enforcement. The government should consider how they are bringing the data together across these organisations to create tangible, meaningful and actional data sources for government and industry and then identifying where data gaps could still lie. This information can help broaden the identification and disruption of ransomware actors and networks. One techUK member highlighted the intel that can be drawn from the publication style from the U.S. Office of Foreign Assets Control (OFAC). They publish the sanctioned actors along with crypto asset address. This information can be used by analytics companies among others, to locate bad actors that could be unknowingly facilitated by certain exchanges or wallet providers. This is a powerful feedback loop which could be replicated in the UK.

One techUK member suggested that organisations are incentivised by reporting using very simple, limited information which they may have available after an attack. Once they have engaged with the governments reporting mechanisms they would then be allowed to interact with the attacker.

One techUK member noted that government should take learnings from the CiSP. CiSP, which was managed by the NCSC, had a voluntary incident reporting scheme. Membership of CiSP was entirely voluntary. With the introduction of NIS some operators of essential services were mandated to report incidents, there was a measurable decrease in the volume of voluntary incidents being shared, resulting in CiSP incident reporting mechanisms being removed. The reason for this was that there were only so many hours in the day, if organisations must report incidents, they will share the minimum rather that all of the useful information they might have voluntarily shared. If organisations feel that they be found liable for a breach based on the information they share, they will be more careful with the information they share. The Cybersecurity Information Sharing Act (CISA) 2015 promotes the proactive sharing of cyber threat information while providing liability protections for entities that share information.[3] There is a tension against useful voluntary information sharing in sectors and across sectors. techUK members noted that mandatory reporting can create tensions on liability and effort in the day, an issue which is exacerbated for SMEs.

Q34. Do you think these compliance measures need to be tailored for different organisations or individuals?

[✓ 1 □ Yes]
2 □ No
If yes, please provide more details on how you think they should be tailored for different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

Question was answered in Q24.

Q35. What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime? *Please select all that apply.*

1 □ Criminal penalties for non-compliance
2 □ Civil penalties for non-compliance
[✓ 98 □ Other, please specify *[free text]*]
96 □ None [free text]
99 □ Don't know.

Question answered in Q10 and Q15. Reporting needs to be incentivised, but in turn 'non-reporting' should not be punished. A ban on payments may actively discourage reporting unless there are incentives such as reporting unlocking help and support for organisations of any size.

Q36. Do you think these non-compliance measures need to be tailored for different organisations and individuals?

[3] CISA. 2015 (https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf)

1 □ Yes
2 □ No
If yes, please provide more details on how you think they should be tailored for different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

Question was answered in Q15 and Q24. One techUK member suggested tailoring non-compliance measures by type or value of the data entity in question holds and the potential operational impact of unavailability of that data.

Q37. Do you think the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors?
1 □ Yes
2 □ No
99 □ Don't know.

Q38. For the mandatory reporting regime, is 72 hours a reasonable time frame for a suspected ransomware victim to make an initial report of an incident?
1 □ Yes
2 □ No.
99 □ Don't know.
If no, what time frame would you recommend and why? [free text]

Q39. Do you think that an incident reporting regime should offer any of the following services to victims when reporting? Please select all that apply.
1 □ Support from cyber experts e.g., the National Cyber Security Centre (NCSC)/law enforcement
2 □ Guidance documents
3 □ Threat intelligence on ransomware criminals and trends
4 □ Operational updates, e.g. activities law enforcement are undertaking.
98 □ Other, please specify [free text]

Q40. Should mandatory reporting cover all cyber incidents (including phishing, hacking etc.), rather than just ransomware?
1 □ Yes
2 □ No
99 □ Don't know