THE RANSOMWARE ATTACK AGAINST THE IRISH HEALTH SERVICE EXECUTIVE: WHAT ROLE FOR THE LAW IN THE FACE OF GROWING CYBER INSECURITY?

MARIA GRAZIA PORCEDDA
School of Law, Trinity College Dublin
ORCID: 0000-0002-9271-3512

Abstract: In May 2021, the Republic of Ireland underwent a cyber crisis within a health crisis. In the middle of the COVID-19 pandemic, Ireland's Health Service Executive suffered a catastrophic cybersecurity attack reputed to have affected virtually the entirety of the Irish population.

This article discusses the role of the law in two ways. First, the article examines the applicable regulatory framework, which broadly splits into preventative and mitigating measures, and the expectations it places on a range of legal actors: the executive, the Courts, the Data Protection Commission, the Garda Cybercrime Bureau, the National Cyber Security Centre and, in passing owing to limited powers under emergency legislation, the Oireachtas. Secondly, the analysis appraises such legal actors' ability to meet the challenges put before them in light of their powers and their actual capabilities.

The law is only one piece of the complex policy jigsaw puzzle in place to address cybersecurity challenges and respond to the crises that follow from a successful cybersecurity attack. The law is also an imperfect piece as such, in light of the many shortcomings of the applicable European Union, Irish and Common Law. This research reflects on the ability of various legal actors to prevent and successfully respond to attacks both based on such legal shortcomings as well as their concrete operational and jurisdictional setup. In so doing, this enquiry contributes to redressing the known research gap on cybersecurity and cybercrime in the Republic of Ireland and pointing to the continued scarcity of data that hampers legal and public policy analysis.

The article ends by highlighting three pinch points for further investigation. The first is the role of the legal-institutional culture within national regulatory authorities and the desirability of implementing measures that may not be perceived as being 'homegrown'. The second pinch point concerns the State's attitude (and potential leniency) in scrutinising its own conduct. The third is the making available of adequate resources to enable legal actors to discharge their duties.

Keywords: HSE ransomware attack; cybersecurity; security incident; emergency; data security; data breach

I. Introduction[1]

In May 2021, the Republic of Ireland woke up to the news that the Health Service Executive (hereafter HSE), the country's national healthcare service, had been hit by a cybersecurity incident.[2] Havoc was wreaked by a ransomware attack[3] - a portmanteau word, combining 'ransom' and 'malware'[4] – where the attackers encode, ie scramble, the data stored in the computers connected to the affected network, in order to make them unintelligible to legitimate users and extort a payment from the victims. The group demanded a ransom of €16.4 million in cryptocurrency to release decryption keys and keep the data in their possession confidential.[5] The amount of the ransom note, which was not paid, [6] is only a fraction of the total cost of the attack and, although network and information systems were restored after a few months,[7] the HSE is still dealing with the practical and reputational consequences of the incident.

Ransomware attacks against healthcare providers came to the fore after the Wannacry attack, which affected portions of the British healthcare system in 2017.[8] They gained traction during the COVID-19 pandemic and are possibly on the rise.[9] Against this background, the HSE attack stands out for the timing and large-scale nature of the strike,[10] with the incident impacting the whole of the national healthcare system and therefore nearly all residents of the Republic. Furthermore, the HSE is critical infrastructure, ie an asset or system, 'the loss or compromise

---

[1] I am grateful to Jonathan Prunty for research assistance and the editor, attendees of the TCD lunchtime seminar series and Dr Martyn Egan for comments on drafts. As customary, all mistakes are mine. This article is part of the PRECYLI project funded by the Provost's PhD Project Award 2021 and the TRISS Academic Fellowship 2021/2022. The law is correct as stated as of March 2023 (with limited updates relating to cases brough against the HSE dating to May 2023).

[2] National Cyber Security Centre, Ransomware Attack on Health Sector, Updated 16 May 2021 (NCSC 2021) https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf.

[3] Mitre, 'Conti' (Mitre Att&ck 2022) https://attack.mitre.org/software/S0575/. On ransomware, see Lena Connolly and David S. Wall, 'The Rise of Crypto-ransomware in a Changing cybercrime Landscape: Taxonomising Countermeasures' (2019) 87 *Computers and Security*.

[4] Also a portmanteau word for 'malicious software', ie a rogue computer programme.

[5] Gareth Corfield, 'Hospitals Cancel Outpatient Appointments as Irish Health Service Struck by Ransomware. Russia-based Criminals Pick Soft Target in Hope of Easy Gains', Fri 14 May 2021, https://www.theregister.com/2021/05/14/ireland_hse_ransomware_hospital_conti_wizardspider/.

[6] Health Service Executive, 'Cyber-attack and HSE Response', last updated 26 May 2023, https://www2.hse.ie/services/cyber-attack/what-happened/.

[7] For the estimated cost of the attack and the timeline of restoration, see Comptroller and Auditor General, 'Report on the Accounts of the Public Services 2021', Chapter 12 - Financial Impact of cyber-attack (2022), 161, https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf.

[8] William Smart, 'Lessons Learned Review of the WannaCry Ransomware Cyber Attack', Independent Report (United Kingdom Department of Health and Social Care, NHS Improvement and NHS England 2018) https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf. See also S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi and P. Aylin 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS' (2019) 98 *NPJ Digital Medicine* 2, https://doi.org/10.1038/s41746-019-0161-6.

[9] Samuel Stolton, 'Von der Leyen: Chinese Cyberattacks on EU Hospitals 'can't be tolerated', *Euractiv* (24 June 2020), https://www.euractiv.com/section/digital/news/von-der-leyen-chinese-cyberattacks-on-eu-hospitals-cant-be-tolerated/; Pieter Haeck, ''It's getting worse': Irish Hospital Hack Exposes EU Cyberattack Vulnerability', Politico (14 May 2021), https://www.politico.eu/article/irish-hospital-hack-highlights-eus-weak-spots/; Maggie Miller, 'The Mounting Death Toll of Hospital Cyberattacks', *Politico* (28 December 2022), https://www.reuters.com/article/us-czech-cyber-ostrava-idUSKBN21Z1OH; see also PricewaterhouseCooper, 'Conti Cyberattack on the HSE. Independent Post Incident Review' Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team (Pwc, 2021), 6-7 (hereafter 'PwC' and 'Conti Cyberattack on the HSE').

[10] Corfield, 'Hospitals Cancel Outpatient Appointments as Irish Health Service Struck by Ransomware', *The Register* (14 May 2021) (n 5).

of which would have a particularly detrimental impact on the availability or integrity of essential services', 'leading to severe' damage to society.[11] As a designated principal response agency at the forefront of emergency intervention,[12] the incapacitation of the HSE was especially problematic: the HSE attack was a cybersecurity crisis within a health crisis.

Understanding the HSE attack as a cybersecurity crisis within a healthcare emergency forms the backdrop for the present investigation, with three caveats. The first is that Ireland did not formally declare a state of emergency either during the pandemic, even though the Republic's response to COVID-19 bore "some of the hallmarks of emergency thinking, with a heavy reliance on Government action",[13] or during the HSE attack. Secondly, we live in structurally cyber-insecure times, where complete cybersecurity is unattainable: the policy focus has shifted from prevention to resilience.[14] Thirdly, legal capabilities are but one piece of the complex policy jigsaw puzzle put in place to foster cybersecurity and respond to attacks.

Ireland's approach to cybersecurity, which is underpinned by its second national cybersecurity strategy,[15] is hardly unique to the country, insofar as both the adoption of the strategy and most regulation concerning network and information systems originate from EU law. EU cybersecurity law is nascent: policies have historically focussed on offending rather than prevention[16] and proposals geared at setting up a coherent preventative strategy are in the making or not yet in force at the time of writing. The cybersecurity landscape in the Republic of Ireland is further particularised by the delayed transposition of EU cybersecurity law and relevant international law, such as the Council of Europe Cybercrime Convention.[17] Although the Republic's position in international cybersecurity rankings has improved,[18] scrutinising the role of Ireland's legal readiness to face cybersecurity challenges is of paramount importance in light of its role as the 'data capital of Europe'[19] and its ambition to be a digital leader.[20]

This article will investigate legal responses to the crisis, by examining the framework in place to deal with cyberattacks and the role of entities vested by such a framework with relevant powers: the executive, the Oireachtas (the legislature), the National Cybersecurity Centre and Data Protection Commission, the Garda National Cyber Crime Bureau and the Courts as actors vested with powers by such applicable law ('legal actors'). While the lack of publicly available data frustrates any investigation of the effectiveness of legal actors in preventing and

---

[11] Department of Defence, Strategic Emergency Management Framework (2017), 19.
[12] Department of Defence, Strategic Emergency Management Framework (2017), Annex A, n. 26; principal response agencies are defined in 'A Framework for Major Emergency Management' (2006).
[13] Conor Casey, Oran Doyle, David Kenny and Donna Lyons, 'Ireland's Emergency Powers During the COVID-319 Pandemic', Report prepared for The Irish Human Rights and Equality Commission by The COVID-19 Law and Human Rights Observatory (Irish Human Rights and Equality Commission 2021). See also: https://www.jstor.org/stable/pdf/27135635.pdf?refreqid=excelsior%3A8c4ef03aac4e89f42fea78355cd347dd&ab_segments=&origin=&initiator=&acceptTC=1.
[14] See Maria Grazia Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law. A Law, Policy and Technology Analysis* (Hart Publishing 2023), ch 1, (hereafter 'Cybersecurity, Privacy and Data Protection in EU Law').
[15] Government of Ireland, National Cyber Security Strategy 2019-2024 (2019) https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf.
[16] Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (2023) ch 1 and conclusions (n 14).
[17] Council of Europe, Convention on Cybercrime (ETS No. 185), Budapest 23 November 2001.
[18] International Telecommunication Union, Global Cybersecurity Index 2020 (ITU-T 2021), 25.
[19] John Kennedy, 'Ireland is the data capital of Europe, says Google (video)' *SiliconRepublic* (4 February 2016).
[20] Department of Further and Higher Education, Research, Innovation and Science, 'Impact 2030: Ireland's Research and Innovation Strategy' (May 2022), 21, https://www.gov.ie/en/publication/27c78-impact-2030-irelands-new-research-and-innovation-strategy/.

responding to the ransomware attack, the analysis will bring into focus pinch points to help in contextualising the role of legal actors and identify areas of future policy intervention.

In doing this, the article pursues three aims. First, it discusses the role of law at times of crisis, which is the theme of the special issue. The HSE attack was a cybersecurity crisis in a healthcare crisis and triggered the application of emergency frameworks. The article examines the legal framework put in place to respond to the emergency and the responses by legal actors vested by such a framework with relevant powers. Secondly, it is hoped that the article will contribute to the literature on the regulatory responses to data breaches and cybersecurity incidents with an Irish case study on the HSE attack. Apart from work in medical sciences studying the disruption of the HSE attack to medical services,[21] legal research by Halder, Gallagher and Murphy has mentioned the attack only in passing.[22] Thirdly, the article aims to help redressing the known research gap on cybersecurity law and policy in Ireland in general[23] and lay the foundations for further research on Ireland's preparedness to deal with cybersecurity incidents. By examining the legal framework and the actions of legal actors, the article will frame Ireland's approach in the context of EU and international cybersecurity law and policy and identify pinch points for future policy intervention.

To pursue these aims, the article draws on several methods. The storyline and main features of the case study rely on desktop research, primarily of governmental reports, news stories around the attack and the PricewaterhouseCoopers' (hereafter PwC) HSE post-incident review. The examination of the legal framework will draw from the legal analysis of primary sources and secondary sources on cybersecurity, cybercrime and data protection law. The mapping of stakeholders and the institutional framework within which they operate takes inspiration from public policy research methods.[24] In the absence of scholarship discussing the legal implications of other cyberattacks in Ireland and thus limited publicly available data, this article draws on grounded theory to identify inductively relevant literature for future research.[25]

---

[21] See Aileen Flavin, Eve O'Toole, Louise Murphy et al., 'A National Cyberattack Affecting Radiation Therapy: The Irish Experience' (2022) 7 *Advances in Radiation Oncology* 5; Clare Faul, Jacqueline Robinson, Jennifer Carey et al., 'Effect of the Cyberattack Targeting the Irish Health System in May 2021 on Radiation Treatment at St. Luke's Radiation Oncology Network' (2022) 7 *Advances in Radiation Oncology* 5; Peter Daly, '"Writing on a curved surface" The Operational Response to the Cyber-attack on the Irish Health Service / « Écrire sur une Surface Courbe» La Réponse Opérationnelle à la Cyber-attaque contre le Service de Santé Irlandais' (2022) 6 *Médecine de Catastrophe – Urgences Collectives* 4; Margaret Moran Stritch, Michael Winterburn and Frank Houghton, 'The Conti Ransomware Attack on Healthcare in Ireland: Exploring the impacts of a Cybersecurity Breach from a Nursing Perspective' (2021) 16 *Canadian Journal of Nursing Informatics* 3-4; Frank Houghton, Letter 'Cybersecurity, Ransomware Attacks and Health: Exploring the Public Health Implications of the Recent Cyberattack on Ireland's Health Service' (2021) 29 *Medicina Internacia Revuo* 116 https://interrev.com/mir/index.php/mir/article/view/176.

[22] In passing: Samprity Halder, 'Cyber Terrorism: A Threat to Human Society' (2022) 3 *Jus Corpus LJ* 1 175; in the context of hacking back: Hannah Gallagher, 'Recognising a Right to Hack Back - Tom and Jerry in Cyberspace?' (2022) 25 *Trinity College Law Review*, 56-82; in the context of financial services: Finbarr Murphy, 'Digital Financial Services, Crypto-assets, Cybersecurity and Regulation' (2022) 29 *Commercial Law Practitioner* 59.

[23] T.J. McIntyre, 'Cybercrime: Towards a Research Agenda' in Deirdre Healy and others (eds*), Routledge Handbook of Irish Criminology* (Routledge 2015); Sheelagh Brady and Caitríona Heinl, 'Cybercrime: Current Threats and Responses. A Review of the Research Literature', Department of Justice and Equality (2020).

[24] Ann Majchrzak and M. Lynne Markus, *Methods for Policy Research: Taking Socially Responsible Action*, (Sage Publications, 2017), ch 2.

[25] Juliet Corbin and Anselm Strauss, 'Grounded theory Research: Procedures, Canons, and Evaluative Criteria' [1990] 13 *Qualitative Sociology*.

The article is organised as follows. Section II summarises the details of the HSE attack. Section III examines the legal framework that applies to the prevention, response and recovery from cyber security incidents and from personal data breaches affecting a critical public sector entity and scrutinises inductively areas of strengths and weaknesses in the applicable Irish legal framework. It furthers maps the field of relevant legal actors, discusses their powers in light of the applicable law, and identifies pinch points affecting the operation of such legal actors. The last section draws conclusions and identifies areas of further research to investigate Ireland's preparedness to deal with cyberattacks.

II. Summary of the HSE attack

The HSE was affected by a Conti ransomware attack[26] attributed to Wizard Spider, a Russia-based cybercrime group.[27] As in a typical ransomware - a portmanteau word, combining 'ransom' and 'malware'[28] – WizardSpider members encoded, ie scrambled, the data stored in the devices connected to the HSE network in order to make them unintelligible to legitimate users and extort the victims. The group demanded a ransom of € 16.4 million in cryptocurrency to release decryption keys and keep the data in their possession confidential,[29] a ransom which does not seem to have been paid.[30]

According to the National Cyber Security Centre, the ransomware attack affected extensive portions of the HSE network before the intervention team shut down all network systems, comprising some 70,000 computers, to prevent the infection from spreading further.[31] Consequently, the HSE network as such became inoperable, effectively forcing personnel to work with pen and paper.[32] Nobody seemingly died in connection to the incident, unlike the Doppelpaymer ransomware attack against the University Hospital Düsseldorf in Germany in September 2020. There, a lady who required urgent care died while being transferred from the hospital's emergency department (which had closed down due to the attack) to the nearest hospital.[33] However, the Conti ransomware attack undermined the ability of the HSE to provide timely care, at a time of ongoing severe pressures caused by the COVID-19 pandemic.[34] Severe

[26] Mitre, 'Conti' (Mitre Att&ck 2022) https://attack.mitre.org/software/S0575/.
[27] Corfield, 'Hospitals Cancel Outpatient Appointments as Irish Health Service Struck by Ransomware' (2021) (n 5); Mitre, 'Wizard Spider' (Mitre Att&ck 2021), https://attack.mitre.org/groups/G0102/.
[28] Also a portmanteau word for 'malicious software', ie a rogue computer programme.
[29] Corfield, 'Hospitals Cancel Outpatient Appointments as Irish Health Service Struck by Ransomware (2021) (n 5).
[30] Health Service Executive, 'Cyber-attack and HSE Response' (n 6).
[31] National Cyber Security Centre, Ransomware Attack on Health Sector, Updated 16 May 2021 (NCSC 2021) https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf. Comptroller and Auditor General, 'Report on the Accounts of the Public Services 2021' (2022) 157 (n 7).
[32] Jack Horgan-Jones, Sarah Burns, Conor Lally and Paul Cullen, 'Bitcoin Ransom Will not Be Paid Following the Cyber-attack on HSE Computer Systems', *The Irish Times* (14 May 2021), https://www.irishtimes.com/news/health/bitcoin-ransom-will-not-be-paid-following-cyber-attack-on-hse-computer-systems-1.4564957; See also Moran Stritch, Winterburn and Houghton, 'The Conti Ransomware Attack on Healthcare in Ireland' (2021) 16 *Canadian Journal of Nursing Informatics* 3-4.
[33] Gareth Corfield, 'Doppelpaymer Ransomware Crew Fingered for Attack on German Hospital that Caused Death of a Patient. Same Mob Promised not to Target Healthcare Facilities', *The Register* (23 September 2020), https://www.theregister.com/2020/09/23/doppelpaymer_german_hospital_ransomware/; William Ralston, 'The Untold Story of a Cyberattack, a Hospital and a Dying Woman. German Prosecutors Tried to Prove that a Ransomware Attack on a Hospital Was to Blame for Someone Losing Their life. Their Story is a Warning', *Wired* (11 November 2020) https://www.wired.co.uk/article/ransomware-hospital-death-germany.
[34] Comptroller and Auditor General, 'Report on the Accounts of the Public Services 2021'(2022) (n 7).

delays lingered even after the Wizard Spider group unexpectedly released the decryption keys, as decrypting a network of such a scale takes several months.[35]

Not only did the attack greatly undermine care, but also it put at risk both personnel data and healthcare records of a number of patients potentially coinciding with the entirety of the Republic's population, which was 5,1 million people based on 2022 census data.[36] As rumours of scams started spreading,[37] the HSE sought and obtained an injunction against persons unknown to restrain the publication of ransomed data.[38] In December 2021, the Garda Síochána intervened when ransomed data was found on sale on illicit data markets on the dark web.[39] At the time of writing, 90,000 individuals have been known to be affected and are in the process of being notified.[40]

In its independent post-incident review commissioned by the HSE in 2021, PwC found that WizardSpider had infiltrated the HSE network by compromising a user's credentials through a phishing email attack, had moved laterally within the network for two months and had eventually mounted the attack by exploiting widespread software vulnerabilities[41] caused by legacy systems, including Microsoft Windows Server 2003.[42] The incident is estimated to have cost the Republic over a hundred million euros.[43]

III. Legal actors' responses to the HSE cyber-attack

This section investigates the responses to the HSE attack as an emergency. Here emergency is not to be understood in its constitutional sense, but rather in the light of frameworks that have been created to deal both with 'emergencies' at large[44] and 'cyber' emergencies. Such a framework includes the blueprint for emergency management, instruments laying down measures for the prevention and mitigation of cybersecurity incidents and personal data breaches (hereafter 'cybersecurity breaches') and laws addressing cybercrime. A critique of the rationales of such legal frameworks, including in a comparative sense, can be found

[35] Recovery lasted until September 2021: PwC 'Conti Cyberattack on the HSE' (2021), 9 (n 9); Comptroller and Auditor General, 'Report on the Accounts of the Public Services 2021' (2002), 163 (n 7).
[36] There does not seem to be a definite figure for HSE patients. For a proxy, see Central Statistics Office, United Nations Sustainable Development Goals, Report on Indicators for Goal 3 Good Health and Well-Being (2019), https://www.cso.ie/en/releasesandpublications/ep/p-sdg3/irelandsunsdgs2019-reportonindicatorsforgoal3goodhealthandwell-being/healthcare/; Central Statistics Office, Census of Population 2022 – Preliminary Results (2022), https://www.cso.ie/en/csolatestnews/presspages/2022/censusofpopulation2022-preliminaryresults/.
[37] Pat Flanagan and Cate McCurry, 'Fears Data Leak from HSE Hack has Begun as Reports of Fraud Calls Begin to Circulate', *Irish Mirror* (24 May 2021), https://www.irishmirror.ie/news/irish-news/fears-data-leak-hse-hack-24176617.
[38] *Health Service Executive v Persons Unknown* [2021] IEHC 75 IA, https://assets.hse.ie/media/documents/order-perfected-20-may-2021.pdf.
[39] Conor Gallagher, 'Garda Specialists Tracked Stolen HSE Data to Commercial Server in US', *The Irish Times* (22 December 2021), https://www.irishtimes.com/news/crime-and-law/garda-specialists-tracked-stolen-hse-data-to-commercial-server-in-us-1.4761457. For an overview of data markets:
[40] Health Service Executive, 'Cyber-attack and HSE Response' (2023) (n 6).
[41] PwC, 'Conti Cyberattack on the HSE' (2021) (n 9).
[42] Comptroller and Auditor General, 'Report on the Accounts of the Public Services 2021' (2022) 163 (n 7).
[43] Michael Brennan, 'Cost of HSE cyberattack to hit 'an eye-watering' €144 million', *Business Post* (14 May 2023) https://www.businesspost.ie/politics/cost-of-hse-cyberattack-to-hit-an-eye-watering-e144-million/.
[44] Emergency is defined in Department of Defence, Strategic Emergency Management. National Structure and Framework (Defence Forces Printing Press 2006), 2.

elsewhere and will only be mentioned in this article[45] to the extent necessary to critically discuss Ireland's legal and policy approach.

The focus of this section is an analysis of legal responses to the crisis by the main actors provided by the applicable law with relevant powers: the executive, the National Cybersecurity Centre and the Data Protection Commission, the Garda Cybercrime Bureau and the Superior Courts. The section also addresses in passing the role of the Oireachtas (the Irish legislature). The analysis of the responses by legal actors focuses on two sets of measures: those taken to minimise the risk of attacks and those taken to mitigate attacks and recover from them. The lessons we can take apply equally to strategies for minimization and mitigation and thus apply transversally to administrative, civil and criminal law as well as the legal-policy divide.

III.i Before the HSE attack: prevention, preparedness and the law

Measures governing the prevention of cybersecurity breaches and preparedness draw primarily from EU law. The chief measures are the Data Protection Act 2018 transposing the General Data Protection Regulation (GDPR) into Irish Law,[46] S.I. No. 360 of 2018, which is the Statutory Instrument transposing the Network and Information Systems Directive into Irish law[47] and the Strategic Emergency Management Framework and related guidelines giving effect to Directive 2008/114/EC (now repealed by Directive 2022/2557[48]) on critical infrastructure, ie infrastructure that is crucial to the functioning of society.

The data protection and Network and Information Systems Directive frameworks are in many ways complementary and follow a similar approach insofar as the prevention of cybersecurity breaches is concerned. Broadly speaking, the two frameworks primarily address entities that decide the objectives and means for processing personal data ('data controllers') and that rely on network and information systems for the provision of their services ('operators' and 'service providers'). Such entities face the obligation, often referred to as a 'duty of care',[49] to adopt

[45] The author's own views can be found in Maria Grazia Porcedda, 'Patching the Patchwork: Appraising the EU Regulatory Framework on Cyber Security Breaches' (2018) 34 *Computer Law and Security Review* 1077 (hereafter 'patching the patchwork'); Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (2023), ch 6 (n 14). Among scholars who wrote on the matter, see Bernold Nieuwesteeg and Michael Faure 'An analysis of the effectiveness of the EU data breach notification obligation' (2018) 34 *Computer Law & Security Review* 6; Michels, Johan David and Walden, Ian, Beyond '"Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?' (2020) 45 *European Law Review 1.*

[46] Data Protection Act 2018 Number 7 of 2018; Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJL 119/1.

[47] S.I. No. 360 of 2018, European Union (Measures For a High Common Level of Security of Network and Information Systems) Regulations 2018; Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1. This article does not include the NIS2 revisions as the revised Directive was still at bill stage at the time of the attack.

[48] Department of Defence, 'Strategic Emergency Framework', Office of Emergency Planning (Defence Forces Printing Press 2017); Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJL 345/75; Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2022] OJL 333/164.

[49] Paul W.J. Verbruggen, Pieter Wolters, Mireille Hildebrandt, Carla Sieburgh, Corjo Jansen, 'Towards Harmonised Duties of Care and Diligence in Cybersecurity' in European Foresight Cyber Security Meeting 2016

state of the art technical and organisational measures, so as to protect data, network and information systems in a way appropriate and proportionate to the security risks to which entities are exposed.

The legal architecture creates positive and negative incentives to protect systems and data, incentives that are weakened by the fact that, at the time of the HSE attack, responsibility to choose technical and organisational measures rested entirely on the responsible entities without being matched by equivalent obligations for technical and organisational measures developers to produce 'cybersecure' systems and mechanisms to verify the adequacy of their security.[50] Under the Strategic Emergency Management Framework, the owners or operators of critical infrastructure are tasked with the responsibility of safeguarding it.[51]

Pursuant to the Strategic Emergency Management Framework and Network and Information Systems Directive, the HSE is both a critical infrastructure and an operator of essential services.[52] Under Regulation 17(1)(b) of S.I. No. 360, an operator of essential services must adopt appropriate technical and organisational measures to prevent and minimise the impact of incidents undermining the provision of essential services. The Minister for the Environment, Climate and Communications - thus the executive - is the competent authority for the security of network and information systems in respect of operators of essential services in the field of Health, the HSE being one such operator.[53] The operational arm of the Department of the Environment, Climate and Communications is the National Cybersecurity Centre, which was founded in 2011 and encompasses the State's National/Governmental Computer Security Incident Response Team.

The National Cybersecurity Centre provides 'early warnings, alerts, announcements and dissemination of information about risk and incidents to relevant stakeholders' and promotes the adoption and use of 'common or standardised practices' for 'incident and risk handling procedures', as well as 'incident, risk and information classification schemes'.[54] Pursuant to Regulation 25 of S.I. No. 360, the National Cybersecurity Centre has published guidance to facilitate the compliance by operators of essential services with the applicable law.[55] S.I. No. 360 lays down a number of offences which can lead to fines of up to half a million euros, but disrespect of duty of care obligations is not an offence. Guideline 3 on Critical Infrastructure Resilience [56] also covers relevant measures, but Version 1 – which was the version in force at the time of the attack - is not publicly available.

(2016), 82-89 https://research.tilburguniversity.edu/en/publications/towards-harmonised-duties-of-care-and-diligence-in-cybersecurity.

[50] As discussed in Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (2023), ch 6 (14).

[51] Department of Defence, Strategic Emergency Management Framework (2017), §4.31, 19 (n 48).

[52] According to PwC (2021) (n 9), the identification took place in 2016, with the NIS Compliance Guidelines for Operators of Essential Service. Governmental sources show that the latter was first published in draft form for public consultation in November 2017 and the first version was adopted on 15 August 2019: https://www.gov.ie/pdf/?file=https://assets.gov.ie/231215/07d2f403-37e9-4916-8519-2f0b609e14d1.pdf#page=null. Note that the NIS Compliance Guidelines predate the entry into force of the Regulations. PwC, 'Conti Cyberattack on the HSE' (2021) (n 9).

[53] SI 360, Reg. 7 (1) (a) and (b).

[54] SI 360, Reg. 10(2) (b), (d) and (g).

[55] National Cybersecurity Centre, NIS Compliance Guidelines for Operators of Essential Service (OES) (Department of Communications, Climate Action and Environment 2019).

[56] Published in July 2021: Department of Defence, Strategic Emergency Management Framework. Guideline 3 – Critical Infrastructure Resilience (Version 2), Office of Emergency Planning (Defence Forces Printing Press 2021). Version 1 has been requested.

In contrast to the National Cybersecurity Centre, the Data Protection Commission has fully-fledged advisory and supervisory powers vis-à-vis data controllers bound by data protection legislation.[57] The HSE is one such data controller and processes, among other, data relating to health: these are special categories of personal data that, on account of the risks they pose to the rights and freedoms of the individuals they relate to, benefit from reinforced protection.[58] The data controller is responsible and accountable for the adoption of technical and organisational measures adequate to the risks threatening such data.[59] Failure to secure the data can result in a hefty financial penalty, which is however limited to €1,000,000 for public authorities, such as the HSE.[60]

At this stage, the Courts and the Garda Síochána play little or no role. Conversely, the executive plays a significant, if indirect role, through the bodies discharging National Cybersecurity Centre or Computer Security Incident Response Team functions and ensuring preparedness through the Strategic Emergency Management Framework, insofar as the responsibility to oversee emergency planning rests on relevant governmental departments and ministers.[61]

Apart from its contribution to EU lawmaking and the transposition of EU law, the legislature plays a limited role at this stage. The regulatory architecture of cybersecurity breaches follows a co-decision, multi-stakeholder model in which the determination of the state of the art is left to the market and international standardisation efforts.[62]

In its post-incident analysis, PwC found that the HSE

"[did] not possess the required cybersecurity capabilities to protect the operation of the health services and the data they process, from the cyber-attacks that all organisations face today. It [did] not have sufficient subject matter expertise, resources or appropriate security tooling […] There were several missed opportunities to detect […] the ransomware".[63]

Notwithstanding the shortcomings of a legal framework tied to a market-based concept of the state of the art in cybersecurity, which resulted in a lack of binding lists of technical and organisational measures required for securing data, network and information systems, the post-incident analysis showed in a matter-of-fact manner a failure on the part of the HSE to meet its duties of care. Indeed, the HSE had overlooked the most basic norms of cyber-hygiene [64] and had not heeded the lessons of incidents suffered by other healthcare organisations: outdated (unsupported) Microsoft software had notably been exploited by the Wannacry ransomware attack affecting the NHS in 2017.[65]

---

[57] Data Protection Act 2018, Parts 2, 6.
[58] Data Protection Act 2018, § 45.
[59] GDPR, Arts 5(2), 25, 32, 33.
[60] Data Protection Act 2018, § 141 (4).
[61] See further, section III.ii.
[62] Maria Grazia Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law* (2023), ch 1 and 6 (n 14).
[63] PwC, 'Conti Cyberattack on the HSE' (2021), 10 (n 9).
[64] PwC, 'Conti Cyberattack on the HSE' (2021), 47-64 (n 9). Paul Cullen, 'HSE Computers Only Monitored for Viruses During Daytime Hours Prior to Cyberattack, Report Reveals' The Irish Times (30 September 2022), https://www.irishtimes.com/news/ireland/irish-news/hse-was-in-uniquely-vulnerable-position-at-time-of-cyberattack-smyth-1.4680803.
[65] Notably Windows XP, William Smart, 'Lessons Learned Review of the WannaCry Ransomware Cyber Attack', Independent Report (United Kingdom Department of Health and Social Care, NHS Improvement and NHS England 2018), 5 https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf.

The PwC post-incident analysis pointed to the absence of adequate capabilities and governance structures within the HSE. Compliance with statutory duty of care obligations, in the guise of the Network and Information Systems Directive (but not S.I. No. 360), standards, codes of conduct and data management, was one among many factors reviewed, but PwC conducted the review in the light of its proprietary incident review system. As one regulatory shortcoming, PwC found that the HSE had last completed its operator of essential services return for the purposes of compliance with the Network and Information Systems Directive two years prior to the accident.[66]

Regulatory responsibilities outside of the HSE were beyond the remit of the PwC post-incident review. Murphy has noted that the PwC report does not refer to the Minister as the competent authority, "and there is no indication that he intervened in that capacity".[67] Before and during the HSE attack, the post of director of the National Cybersecurity Centre was revamped to match the significance of cybersecurity in contemporary societies.[68] At the time of the HSE attack, the Data Protection Commission was under scrutiny over its ability to discharge its supervisory functions.[69] Such circumstances beg the question of whether the conditions under which legal actors discharge their statutory duties could affect the preparedness of Operators of Essential Services, such as the HSE; at the time of writing, there is insufficient data to establish any such links. The circumstances affecting legal actors thus constitute a first pinch point for further research and potential intervention.

III.ii After the HSE attack: mitigation, recovery and the law

The law applicable to the mitigation of and recovery from cybersecurity breaches includes sectoral rules transposing EU law, such as the abovementioned DPA 2018, S.I. No. 360 and the Criminal Justice (Offences Relating to Information Systems) Act 2017,[70] as well as Irish law generally. In addition to the Constitution and common law, statutory measures of relevance are those empowering Courts to grant injunctions and instruments vesting the Garda Síochána with investigatory and prosecutorial powers.

The Strategic Emergency Management Framework specifies the chain of command during an emergency and consequently identifies legal authorities and frameworks. Emergency management policy and activities are coordinated by the Government Task Force on Emergency Planning, which "is chaired by the Minister for Defence and comprises senior

---

[66] PwC, 'Conti Cyberattack on the HSE' (2021), 97 (n 9).
[67] Murphy, 'Digital Financial Services' (2022), 76 (n 22).
[68] Blathnaid O'Dea, 'New Director to Lead Ireland's National Cyber Security Centre', *Silicon Republic* (27 January 2022), https://www.siliconrepublic.com/enterprise/government-appoints-new-director-of-national-cyber-security-centre. Recommendations to have the NCSC report to the National Security Coordinator instead of the Department of Communications, Climate Action and Environment do not seem to have been followed. See Commission on the Future of Policing in Ireland, 'the Future of Policing in Ireland' (2018), 37, https://www.gov.ie/pdf/?file=https://assets.gov.ie/180551/8b6b5065-5720-4a24-a40c-a2b15446770c.pdf#page=null.
[69] House of the Oireachtas Joint Committee on Justice, Report on meeting on 27th April 2021 on the topic of GDPR (2021), 33/JC/06, https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_justice/reports/2021/2021-07-22_report-on-meeting-on-27th-april-2021-on-the-topic-of-gdpr_en.pdf.
[70] Transposing Directive 2013/40/EC of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJL 218/8.

representatives of all Departments".[71] A sub-group deals with critical infrastructure, but the version of the guidelines that was in force when the attack occurred was unavailable at the time of writing, so that what follows draws from the overarching Strategic Emergency Management Framework instead.

National-level emergency coordination of communications services and network and information systems is coordinated by the Lead Government Department, currently called the Department for the Environment, Climate and Communications, in conjunction with other relevant government department and agencies.[72] 'Principal supporters' for network and information systems emergencies include the Computer Security Incident Response Team ('CSIRT-IE') within the Department for the Environment, Climate and Communications, the Government Chief Information Office, an Garda Síochána, the Commission for Communications Regulation, the Department of Defence and Department of Business, Enterprise and Employment systems operators, users and providers.[73] Stakeholder cooperation is considered to be particularly desirable by the European Judicial Cybercrime Network in the aftermath of ransomware incidents.[74] The post-incident recovery investigation has pointed to the early prominence of private parties, the defence forces, an Garda Síochána and the National Cybersecurity Centre in the early stages of the attack, with defence forces' intervention then being phased out a few weeks after the incident.[75] Interpol was engaged,[76] as, reportedly, was Europol.[77]

Coordination thus rests with the public administration, under executive (ie departmental and ultimately ministerial) leadership, with the Taoiseach and ministers being regularly briefed.[78] The Oireachtas should also receive relevant briefing material, but Oireachtas debates on ongoing emergencies are subordinate to "the resource implications for the lead Department and first responders in servicing such a debate",[79] and thus may be deferred. The legislature is therefore expected to take a step back in emergencies. It is worth noting that the PwC post-incident review does not mention the Oireachtas and related Irish applicable law.

The applicable cybersecurity and data protection law lays down rules for the response to cybersecurity breaches; remedial avenues are disciplined by a blend of EU, Irish statutory and common law measures.[80] A cyberattack such as that suffered by the HSE can yield multiple tiers of victims, with the primary victim being the breached entity, secondary victims being the individuals whose personal information and health is negatively affected, and tertiary victims being individuals who may be harmed in connection with, but independently from, primary

71 Department of Defence, Strategic Emergency Management Framework (2021), 6 (n 56).
72 The relevant LDG for pandemics is the Department of Health, Department of Defence, 'Strategic Emergency Management Framework' (2017), 10 and Annex A, n. 26 (n 48). Otherwise, emergency coordination "is generally led by the relevant officials/experts", ibid, 13.
73 Department of Defence, Strategic Emergency Management Framework (2017), Annex A, n. 7 (n 48). An additional agency is IDC on Cyber Security, but the acronym is not explained.
74 European Judicial Cybercrime Network, 'Cybercrime Judicial Monitor. Issue 7' (Eurojust 2022), 17-26.
75 PwC, 'Conti Cyberattack on the HSE' (2021), 9 (n 9).
76 Ibid, 139, citing meeting minutes.
77 Dan Grennan, 'New Cyber-attack Carried out on Department of Health as HSE Scrambles to Get Systems Back Online', *Extra.ie* (16 May 2021), https://extra.ie/2021/05/16/news/irish-news/ransomeware-health-department; subsequently: Colman O'Sullivan, 'IT infrastructure of crime group 'significantly disrupted' by gardaí', *RTE* ((5 September 2021), https://www.rte.ie/news/ireland/2021/0905/1244805-cyber-attack-gardai/.
78 Department of Defence, Strategic Emergency Management, (2017), 11 (n 46).
79 Ibid, 13; also PwC 'Conti Cyberattack on the HSE' (2021), detailed organisational timeline, 138-141 (n 9).
80 See generally, Michael O'Doherty, *Internet Law* (Bloomsbury Professional 2020).

and secondary victims.[81] In the case of the HSE attack, there is evidence of primary and secondary victimisation, a point discussed below.

Cybersecurity and personal data protection laws target the entity breached as a potentially 'negligent victim', insofar as their responsibility in causing the incident is scrutinised in post-incident assessments and may give rise to administrative or criminal liability. The Network and Information Systems Directive and GDPR frameworks require a breached entity to report the incident to the National Cybersecurity Centre and the Data Protection Commission within stringent timelines.

The PwC post-incident review contains evidence to the effect that the HSE Data Protection Officer launched a data protection investigation, in cooperation with an Garda Síochána, so as to notify a personal data breach to the Data Protection Commission within the statutory timeline.[82] At the time of writing there is no evidence of a Data Protection Commission fine having been levied against the HSE pursuant to section 111 of the Data Protection Act 2018. The fact that, according to the post-incident review, the HSE did not adopt the most basic security measures suggests there may have been a breach of the confidentiality and security data protection principle enshrined in Art 5(1)(f) GDPR, which should attract the highest level of fine.[83] The PwC review points to the HSE's timely notification of the breach to the National Cybersecurity Centre.[84] A failure to do this could have incurred fines pursuant to Regulation 34 of S.I. No. 360. It should be noted that, had this happened, the State would have been issuing penalties for its own statutory misconduct, under rules derived from EU law. A relevant question is whether sufficient incentives exist to secure the efficient enforcement of rules that are derived from EU law rather than 'homegrown'. Two separate pinch points may be identified here: the incentive for the state to take action against itself, and the incentive to implement measures that are not strictly 'homegrown'.

The fact of being, institutionally and individually, the victim of an attack that meets the definition of multiple offences attracts the application of Irish administrative, criminal and evidence laws, read in light of the Constitution and the common law. Cybersecurity breaches and ransomware attacks trigger the application of a range of criminal law provisions. In addition to offences created by Regulations 18, 22, 29, 30, 31 and 33 of S.I. No. 360, key substantive cybercrime offences are also found in the Criminal Justice (Offences Relating to Information Systems) Act 2017, in sections 1 and 2 of the Criminal Damage Act, 1991 and in sections 9 and 25 of the Criminal Justice (Theft and Fraud Offences) Act 2001.[85]

Investigations are carried out by the Garda Síochána in line with the Criminal Evidence Act 1992[86] and a host of other instruments.[87] Prosecutorial powers lie primarily with the Director

[81] See generally Maria Grazia Porcedda and David S. Wall, 'The Chain and Cascade Effects in Cybercrime' (IEEE Euro S&P 2019); Maria Grazia Porcedda, 'Sentencing Data-driven Cybercrime. How Data Crime with Cascading Effects is Tackled by UK Courts' (2023) 48 *Computer Law & Security Review*.

[82] PwC, 'Conti Cyberattack on the HSE' (2021), 84 and detailed organisational timeline, 138-141 (n 9).

[83] GDPR, Arts 82-3.

[84] PwC, 'Conti Cyberattack on the HSE' (2021), detailed organisational timeline, 138-141 (n 9).

[85] For a pre-2017 review, see McIntyre, 'Cybercrime: Towards a Research Agenda' (2015), n 23; see also Paul Johnstone, 'Cybercrime and the law: a critical review of current legisaltive provisions to tackle cybercrime' (Trinity College Dublin 2015). NB §2 of the Criminal Damage Act, 1991, classes data as property.

[86] Currently under review, see below.

[87] Other instruments include the Criminal Justice Act 2006 and 2011; "identification of the extent and scope of the powers of the Gardaí [is] a challenge which is grappled with by Gardaí and practitioners alike": Rebecca Coen, *Garda Powers: Law and Practice* (Clarus Press 2014).

of Public Prosecutions (DPP) and secondarily with the Garda and are disciplined by the Prosecution of Offences Act 1974 and the Garda Síochána Act 2005.[88] Remedial avenues beyond the statutory powers created by cybersecurity breach legislation apply. Courts' powers are overseen by Articles 34-37 of the Constitution and S.I. no. 15/1986 on the Rules of the Superior Courts.[89] Relevant legal actors are the Garda Síochána and especially its National Cyber Crime Bureau (GNCCB), the Director of Public Prosecutions (DPP) and the Superior Courts. Here the focus is on the Garda National Cyber Crime Bureau and Courts.

The response to ransomware attacks and cybersecurity breaches follows classic criminal justice approaches. Although Directive 2013/40 contains no specific 'ransomware' offence, the combination of provisions drawn from the Directive and other instruments have been deemed by other EU Member States to be sufficient to respond to ransomware attacks[90] and the same may well be the case in Ireland. Such offences are investigated by the Garda National Cyber Crime Bureau with the aim of prosecuting offenders, offering redress to wronged victims and protecting society. However, cybercrime law suffers from known shortcomings and alternative remedial avenues for victims can also prove unsatisfactory.

Redressing the injustice suffered by victims of cybercrime is inherently challenging due to the interplay between the architecture of cyberspace, difficulties in attributing cybercrimes and choosing the appropriate jurisdiction for law enforcement, a situation which gives offenders the upper hand, with knock-on effects on investigations, prosecutions and sentencing.[91] In essence the distributed architecture of the internet enables offenders to obfuscate their identity and, when they happen to be identified, to escape prosecution by exploiting jurisdictional boundaries to their advantage. In the case of ransomware attacks, an additional challenge is that victims may avoid reporting incidents, and when they report them, victims' interest in restoring business continuity can undermine investigatory efforts.[92] Peters' research shows that class actions against entities that have suffered data breaches in the US have not offered much relief to affected data subjects.[93] Such reality must form the background to all critical reviews of HSE-related criminal investigations, prosecutions and case law in Ireland.[94]

---

[88] Prosecution of Offences Act, 1974 (Consolidated) 1974 No. 22 up-to-date to February 9, 2023. For a comprehensive analysis of the Irish law of evidence, see Liz Heffernan, *Evidence in Criminal Trials* (Bloomsbury Professional, 2nd edn, 2020).

[89] The Rules of the Superior Courts 1986, SI 1986/15 https://www.irishstatutebook.ie/eli/1986/si/15/made/en/print; https://www.courts.ie/superior-court-rules.

[90] European Judicial Cybercrime Network, 'Cybercrime Judicial Monitor. Issue 7' (2022), 17-26 (n 74). Additional instruments applicable to cybercrime offences could include the common law offence of Conspiracy to defraud, Non-Fatal Offences Against the Person Act, 1997 Offences Against the State (Amendment) Act, 1998, the Criminal Justice Act, 2006. See Paul Johnstone, 'Cybercrime and the law' (2015) (n 85). Section 19 of the Criminal Justice Act, 2011, creating a statutory duty to report serious offences also applies as 'relevant offences' include most cybercrimes, as discussed by T.J. McIntyre, 'Cybercrime: Towards a Research Agenda' (2015) (n 23).

[91] See generally David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity 2007); Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press 2010); Susan Brenner, *Cyberthreats and the Decline of the Nation-state* (Routledge 2014).

[92] European Judicial Cybercrime Network, 'Cybercrime Judicial Monitor' (2022), 17-26 (n 74).

[93] Rachel M. Peters, So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws' (2014) 56 *Arizona Law Review* 4.

[94] Irish cybercrime law was met with criticism prior to the 2017 reform, most recently by T.J. McIntyre, 'Cybercrime: Towards a Research Agenda' (2015) (n 23) and Johnstone, 'Cybercrime and the law' (2015) (n 85).

After the Financial Times reported that 'stolen' data had appeared online,[95] the HSE brought an action against "persons unknown", ie "those responsible for accessing the [HSE's] IT system and planting a ransomware note thereon discovered by the [HSE] on 14 May 2021" referred to as the 'intended defendants', which was heard in camera and came with reporting restrictions.[96] The HSE was granted injunctions restraining 'intended defendants', but also 'their servants or agents, or any other person having notice of the making of this Order' from profiting from the proceeds of the attack, and interim injunctions directing them to surrender any data in their possession and to identify themselves within a set timeframe. The HSE was further allowed to serve Notice of these proceedings through alternative means and out of the Jurisdiction pursuant to Orders 10, Rule (1) and 11, Rule (1)(f) of the Rules of the Superior Courts 1986.

Very few cybercrime cases have been tried in the Republic of Ireland thus far. In the absence of an Irish precedent on ransomware, practitioners suggest that Courts could draw on English case law for guidance. Besides the interim use of descriptors such as 'persons unknown', for which there are Irish cases,[97] Thullier points to *Novartis Pharmaceuticals UK Ltd v Stop Huntingdon Animal Cruelty* and *Clarkson plc v Person or Persons Unknown* as cases where the identity of defendants remained undetermined.[98] Thullier also cites *LJY v Persons Unknown* and *CMOC v Persons Unknown* as establishing that an IP (internet protocol) address is a sufficient 'tort gateway', ie a way to ground tort proceedings in the jurisdiction.[99] Furthermore, he explains that in English blackmail cases such as *LJY v Persons Unknown* and *ZAM v CFM and TFW*, Courts have granted anonymisation and sat *in camera*.[100] Thullier notes that the orders made in these cases 'can assist in identifying the persons unknown, or at least in providing a piece of the puzzle'.[101]

Although the intended defendants were yet to be identified,[102] the HSE received a decryption key on the evening of 20 May 2021, which significantly contributed to the restoration of HSE

[95] Laura Noonan and James Shotter, 'Irish Patients' Data Stolen by Hackers Appears Online', *Financial Times* (19 May 2021) https://www.ft.com/content/13d33a08-ce83-4f8a-8d93-a60a5e097ed8.
[96] Health Service Executive and Persons Unknown [2021], IEHC 75 (https://assets.hse.ie/media/documents/order-perfected-20-may-2021.pdf).
[97] There exist precedents for the use of the descriptor 'persons unknown': *Digital Hub Development Agency Substituted by Order of the County Registrar for the Commissioners of Public Works in Ireland v Martin Keane and Gerry O'Reilly, The Commissioners of Charitable Donations and Bequests for Ireland and Persons Unknown* [2008] IEHC 22; *KBC Bank Ireland PLC v Gordon Smith, Linda Hussey, Ben Gilroy and Unknown Persons Occupying the Premises at Chieftains Way, 37 Hamlet Avenue, Balbriggan, Co. Dublin* [2018] IECA 90; *Remcoll 2 Limited v Fred Walsh, Gordon Hughes, Ita Reynolds, Bryan Cribben, Adrian Smith, Desmond Wisley and Persons Unknown at the Rock Centre, Ballinamore, County Leitrim* [2019] IEHC 942.
[98] *Novartis Pharmaceuticals UK Ltd v Stop Huntingdon Animal Cruelty* [2014] EWHC 3429 (QB) and *Clarkson plc v Person or Persons Unknown* [2018] EWHC 417 (QB) in A Thullier,'The Value of Sending a Signal to Hackers', *Law Society Gazette* (Return of the Cybermen, 3 April 2020), https://www.lawsociety.ie/gazette/in-depth/cyberattackers. He also mentions *Bloomsbury Publishing Group plc v News Group Newspapers Ltd* [2003] EWHC 1087 (Ch) (https://www.casemine.com/judgement/uk/5a8ff72860d03e7f57ea8d59) for the use of 'persons unknown'.
[99] *LYJ v Persons Unknown* [2017] EWHC 3230 (QB) (https://www.casemine.com/judgement/uk/5b2897ad2c94e06b9e1983df); *CMOC v Persons Unknown* [2017] EWHC 3599, cited in A Thullier (2020).
[100] LYJ v Persons Unknown, *ZAM v CFM and TFW* [2013] EWHC 662 (QB), cited in A Thullier (2020).
[101] Ibid.
[102] Some leads may have been opened up by a data dump in Spring 2022; Cormac O'Keeffe, 'Gardai Trawl Leaked Files of HSE Cyber Gang', *Irish Examiner* (8 March 2022), https://www.irishexaminer.com/news/arid-40823811.html.

services.[103] Thereafter, PwC reported that "Social media monitoring system Talk Walker was set up to scan the web for leaked patient data."[104] The Irish Times reported that after receiving a copy of the High Court order, the Financial Times revealed that 27 files stolen from the HSE were available for download on VirusTotal, a malware analysis service. [105] The Irish Times further reported that in June 2021 the HSE sought 'Norwich Pharmacal' orders against the owners of VirusTotal, Chronicle Security Ireland Ltd and its US-based parent Chronicle LLC, both ultimately owned by Google, to identify the twenty or so people believed to have handled the files on the platform.[106] The data, which included 'correspondence, minutes of meetings, and corporate documents', 'was downloaded 23 times before it was removed on May 25th'[107] 2021, after the malware analysis companies received the order. At the time of writing, the outcome of the proceedings remains unknown.

Practitioners recommend obtaining an injunction in order to show the breached entity understands the gravity of the incident, thus helping to demonstrate to the Data Protection Commission they take their accountability obligations seriously in the context of the notification of a data breach, as well as to dissuade third parties from processing the data further. Enforcement orders may also be needed pursuant to intermediary liability provisions as laid down by the e-Commerce regulations,[108] although only law-abiding online users are likely to be deterred from further processing the data, given that data is a currency for cyber-offenders[109] (and data-hungry corporations).

In September 2021 the Garda National Cyber Crime Bureau 'seized several domains used in the HSE cyber attack'[110] and later in the year was able to retrieve data relating to the attack on a commercial server located in the US, which the US Department of Justice shared with the Director of Public Prosecutions via a mutual legal assistance treaty.[111] Reportedly 'the recovered information is thought to contain a mix of personal data including phone numbers and email addresses, and medical information such as records, notes and treatment histories.'[112]

---

[103] Pwc, 'Conti Cyberattack on the HSE' (2021), 140 (n 9).
[104] Ibid.
[105] Aodhan O'Faolain, 'Cyberattack: HSE seeks court orders to help identify those who accessed stolen files. 20 people uploaded or downloaded confidential data onto a service by Google-owned security' *The Irish Times* (25 June 2021), https://www.irishtimes.com/news/crime-and-law/courts/high-court/cyberattack-hse-seeks-court-orders-to-help-identify-those-who-accessed-stolen-files-1.4603522 (hereafter 'Cyberattack'); see also Health Service Executive ransomware attack, Wikipedia.org, https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack#cite_note-ie-hse-seeks-order-to-find-who-uploaded-or-downloaded-files-66.
[106] Ibid. 'Norwich Pharmacal orders' are disclosure orders used to compel a defendant to release information that will enable a victim to take actions against a wrongdoer.
[107] Deirdre Crowley and Michael Byrne, 'Containing and Combatting Cyber Attacks through the Courts' (Matheson, 5 October 2021), https://www.matheson.com/insights/detail/containing-and-combatting-cyber-attacks-through-the-courts21.
[108] European Communities (Directive 2000/31/EC) Regulations 2003 (SI 68/2003).
[109] See Paul Hunton, 'Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime' (2011) 28 *Computer Law & Security Review* 201, 202; Maria Grazia Porcedda and David S. Wall, 'The Chain and Cascade Effects in Cybercrime: Lessons from the TalkTalk Case Study' (IEEE Euro S&P 2019); Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020.
[110] O'Sullivan, 'IT Infrastructure of Crime Group 'Significantly Disrupted' by Gardaí' (2021) (n 77).
[111] Criminal Justice (Mutual Assistance) Act 2008, Schedule 14, https://www.irishstatutebook.ie/eli/2008/act/7/schedule/14/enacted/en/html; Conor Gallagher, 'Garda Specialists Tracked Stolen HSE Data to Commercial Server in US. Cyber crime Personnel Had Been Tracking Movement of Data for Months', *The Irish Times* (22 December 2021), https://www.irishtimes.com/news/crime-and-law/garda-specialists-tracked-stolen-hse-data-to-commercial-server-in-us-1.4761457.
[112] Conor Gallagher, 'Garda Specialists Tracked Stolen HSE Data to Commercial Server in US', *The Irish Times* (2021).

The data relates to 90,000 individuals or, in data protection law parlance, data subjects. Such 'secondary' ransomware victims are in the process of being notified and about one hundred of them sued the HSE for damages under data protection legislation.[113] It will be for future work to discuss such actions as most cases are expected to stay proceedings, as did Judge John O'Connor at Dublin Circuit Court, pending a determination by the Court of Justice of the European Union of several relevant preliminary references.[114]

Ireland had to rely on a mutual legal assistance treaty to source the unlawful data, in the absence of more agile mechanisms such as those contained in the Council of Europe Cybercrime Convention. Ireland had signed but not ratified the Convention,[115] reportedly due to gaps in the Irish law of evidence that hinder the transposition of procedural provisions of the Convention.[116] Since evidentiary powers were under revision at the time of the attack,[117] the question of whether additional investigative powers might have made a difference is open to speculation. Discussing, however, whether the Garda Síochána having an internal as well as external intelligence gathering role is supportive or detrimental to cyber investigations is beyond the scope of this paper.

Another relevant issue is the persistent question of resourcing, first highlighted by McIntyre,[118] coupled with the difficulty for police forces to recruit in competition with the private sector.[119] The Garda National Cyber Crime Bureau was established in 2017 and is 'tasked with the forensic examination of computer media seized during the course of any criminal

---

[113] Mary Carolan, Up to 100 Cases Taken over HSE Cyberattack, Judge Told', *The Irish Times* (18 May 2023) https://www.irishtimes.com/crime-law/courts/2023/05/18/up-to-100-cases-taken-over-hse-cyberattack-judge-told/.

[114] Ibid. These include: Case C-300/2, *Österreichische Post*, ECLI:EU:C:2023:370 (summary at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-05/cp230072en.pdf); Case C-340/21 – VB v Natsionalna agentsia za prihodite; Case C-667/21 – ZQ v Medizinischer Dienst der Krankenversicherung Nordrhein; Case C-687/21 – BL v Saturn Electro-Handelsgesellschaft mbH Hagen; Case C-741/21 – GP v Juris GmbH; Case C-182/22 – JU v Scalable Capital GmbH. Judge John O'Connor also stayed proceedings in *Gary Cunniam v Parcel Connect Ltd t/a Fastway Couriers Ireland & Others* [2023] IECC 1 (https://ie.vlex.com/vid/gary-cunniam-v-parcel-924139666). See Colin Monaghan, Deirdre Munnelly and Anthony Strogen, 'Defending Data Breach Claims in Ireland. An Update' (Mason, Curran & Hayes, 17 February 2023), https://www.mhc.ie/latest/insights/defending-data-breach-claims-in-ireland-2; Rachel Hayes, Adele Hall and Leo Moore, 'Non-material Damage for Data Protection Breaches before the Irish and EU Courts – Clarity Ahead?' (William Fry, February 2023), https://www.williamfry.com/knowledge/non-material-damage-for-data-protection-breaches-before-the-irish-and-eu-courts-clarity-ahead/. For an analysis predating the GDPR, see Eoin O'Dell, 'Compensation for Breach of the General Data Protection Regulation' (2017) 40 *Dublin University Law Journal*, 1.

[115] Council of Europe, Chart of signatures and ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. MLAT citation.

[116] Houses of the Oireachtas, Debate of Thursday, Cybersecurity Policy (10 September 2020) https://www.oireachtas.ie/en/debates/question/2020-09-10/38/. See also Johnstone, 'Cybercrime and the Law' (2015) (n 85); McIntyre, 'Cybercrime: Towards a Research Agenda' (2015) (n 23); Adrian Bannon, 'Cybercrime Investigation and Prosecution - Should Ireland Ratify the Cybercrime Convention' (2007) 3 *Galway Student Law Review*.

[117] See Joint Committee on Justice, *Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Powers) Bill* (June 2022), https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_justice/reports/2022/2022-06-01_report-on-pre-legislative-scrutiny-of-the-general-scheme-of-the-garda-siochana-powers-bill_en.pdf; Deb 22 Feb 2023, Vol. 1034, No. 1, https://www.oireachtas.ie/en/debates/debate/dail/2023-02-22/23/.

[118] McIntyre, 'Cybercrime: Towards a Research Agenda' (2015) (n 23).

[119] Conor Gallagher, 'Garda Struggling to Tempt Cybercrime Experts from Private Sector', *The Irish Times* (14 July 2021) https://www.irishtimes.com/news/crime-and-law/garda-struggling-to-tempt-cybercrime-experts-from-private-sector-1.4620541.

investigations',[120] thus giving it a very broad remit given the relevance of digital evidence to contemporary offending. The Future of Policing in Ireland Report of 2018 called for an expansion of the Bureau's 'capacity and expertise' 'as a matter of urgency', and to fast-track the recruitment of personnel.[121] In 2021 the Bureau went from having 400 to 459 staff and opened satellite offices, but is still working through a backlog of cases.[122] Allocation of resources is a relevant pinch point for both the prevention and prosecution aspects of cybersecurity breaches. At the time of writing, no suspects have been identified in conjunction with the HSE attack and no charges have been pressed.

In sum, the legislation is but one instrument of intervention after a cyberattack and the fragmentation of the regulatory framework prevents a global assessment at this stage. First responders have been met with praise:[123] their role was arguably supported by the Strategic Emergency Management Framework (SEM). The framework for stakeholder cooperation flowing from the SEM possibly helped reconciling the opposing goals of continuity of service and investigative needs, a sore point in ransomware cases according to the European Judicial Crime Network. Judicially, the common law may also be creating room for creativity.

At the same time, a number of known shortcomings affecting cybersecurity breach and cybercrime instruments may be enhanced by jurisdiction-specific matters, such as the inability to rely on instruments that might have made a difference such as the Budapest Convention. Without detracting from the praise with which first-responders have been met, this analysis has identified pinch points, including gaps in capabilities, that could impact on the ability of legal actors to deliver on their expectations and contribute to the success of the law at times of crisis.

IV. Conclusion. What role for (Irish) law at times of cyberattacks?

This article has analysed the legal responses to the HSE ransomware attack as of Spring 2023. The analysis is *in media res* as further input may come from the Garda National Cyber Crime Bureau and Data Protection Commission, as well as court cases brought against the HSE. The claims contained in this article have thus been qualified accordingly.

The article examined the role of the law at a time of crisis. The HSE attack was a cybersecurity crisis in a healthcare crisis and triggered the application of frameworks created to deal with 'emergencies' in the common sense of the word. In particular, this article has examined the legal framework put in place to respond to cybersecurity-related emergencies, which draws from international, EU and Irish law, both statutory and common law. Such framework includes two broad categories of instruments: instruments of prevention and of intervention. Once the attack was identified, the Strategic Emergency Management Framework seemed to deliver, bringing about multi-stakeholder cooperation of a kind that the European Cybercrime Judicial Network believes to be of essence in ransomware cases. The common law also

[120] An Garda Síochána, 'Garda National Cyber Crime Bureau (GNCCB)' https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/.
[121] Commission on the Future of Policing in Ireland, 'Future of Policing in Ireland Report' (2018), 27 (n 68).
[122] Cormac O'Keeffe, 'Garda Cyber Unit Cases Rise 22% but Backlog Persists', *Irish Examiner* (4 June 2022) https://www.irishexaminer.com/news/courtandcrime/arid-40888037.html. David Looby, 'Wexford Garda Cyber Crime Unit is One of Only Four Units in the Country', *Independent* (24 January 2023), https://www.independent.ie/regionals/wexford/news/wexford-garda-cyber-crime-unit-is-one-of-only-four-units-in-the-country-42307653.html.
[123] See generally PwC, 'Conti Cyberattack on the HSE' (2021) (n 9), with reservations for low levels of pre-incident preparedness at the HSE.

appeared to offer the flexibility required to deal with offences not yet widely tried in the Republic.

However, there is no methodology for assessing the overall impact of the law in such cases. Metrics evaluating post-incident intervention (which for instance assess how many days it takes an organisation to identify a breach and to restore services) aim to estimate costs and are thus of limited help in making claims about the law. Such metrics may even detract from the fact that ransomware attacks point to a failure of the legal system in preventing incidents – if the law ever could.

Indeed, legislation is but one instrument of response to the challenge of cybersecurity and a blunt one as such, due to the known shortcomings of EU and Council of Europe cybersecurity breach and cybercrime instruments. As cyberattacks engender potential 'negligent victimhood' on the part of the primary victim, legal instruments often express conflicting objectives: trying to scrutinise the victim's role in the incident, especially if secondary victims are present, as well as supporting the mitigation of the incident, restoring continuity of service and the protection of all victims concerned. Furthermore, cybersecurity laws have developed haphazardly and are under reform at the time of writing. To this must be added jurisdiction-specific matters, eg delays in the transposition of European Union measures and international instruments, disputed enforcement capabilities, and the common law tradition which creates judicial space for flexibility. In point of fact, the 'light touch' legal obligations which are incumbent upon the HSE for securing network and information systems as an Operator of Essential Service, and which I have criticised extensively elsewhere,[124] have seemed to create insufficient incentives to implement adequate cybersecurity technical and organisational measures, a failure also highlighted by Murphy.[125]

Against this background, the article has also examined the responses by legal actors vested by the legal framework with relevant powers: the executive, the National Cybersecurity Centre and Data Protection Commission, the National Garda Cyber Crime Bureau and the Superior Courts. The article has also showed that the Oireachtas (the legislature), plays a modest role *vis-à-vis* the executive. This may be explained through the national balance of powers between parliament and the executive,[126] as well as the marginalisation of the legislature at times of emergency reflected in the Strategic Emergency Management Framework and inherited from the wars on national and international terror. Research is under way at the time of writing to analyse parliamentary responses in greater details, and it will be for future publications to report on the findings.

This research has highlighted three pinch points that warrant further investigation, also with a view to identifying suitable policy responses. The first is the role of the legal-institutional culture within national regulatory authorities and the desirability of implementing measures that may not be perceived as being 'homegrown'. On this point there are conflicting data: Ireland transposed Directive 2013/40 late, but the latest version of the Strategic Emergency Management Framework anticipates the EU update of the 2008 Directive on critical

[124] Porcedda, 'Patching the Patchwork' (2018) (n 45).
[125] Murphy (2022), (n 22).
[126] See generally Gavin Barrett, 'The Oireachtas and the European Union: the Evolving Role of a National Parliament in European Affairs' (Houses of the Oireachtas, Dublin, 2013); Gavin Barrett, *The Evolving Role of National Parliaments in the European Union: Ireland as a Case Study* (Manchester University Press, 2018); Oran Doyle, *The Constitution of Ireland. A Contextual Analysis* (Hart Publishing 2018), 46-83.

infrastructure.[127] The second pinch point concerns the State's attitude (and potential leniency) in scrutinising its own conduct. The third is the making available of adequate resources to enable legal actors to discharge their duties; the scarcity of data prevents carrying out an appraisal of the effectiveness of legal actors' responses. Such questions are inter-related and cut across multiple debates of administrative law, EU-national law and national regulatory authorities and it will be for further research to untangle them.

This analysis is intended to contribute to the literature on the regulatory responses to data breaches and cybersecurity incidents with an Irish case study on the HSE attack. In so doing, this article contributes to redressing the known research gap on cybersecurity law and policy in Ireland in general[128] and to laying the foundations for further research on Ireland's preparedness to deal with cybersecurity incidents. Without detracting from the praise with which first responders have been met,[129] the analysis has identified pinch points that could detract from the ability of legal actors to successfully prevent and respond to cyberattacks.

This research is therefore one piece of a larger endeavour appraising the state of cybercrime and cybersecurity law and policy in Ireland. The evidence discussed in these pages questions the reconciliation of the state of the HSE with Ireland as the data capital of Europe and the narrative of a high-tech economy.[130]

Although more complete legal frameworks and related capabilities may have improved the response to the attack, we cannot prove a counterfactual. What we can do instead is to build on these questions to create the evidence base to discuss reform and the appropriate locus of that reform. It will be for further research to pursue this enquiry.

[127] See fn 48 and 56 above.
[128] McIntyre, 'Cybercrime: Towards a Research Agenda' (2015) (n 23); Brady and Heinl, 'Cybercrime' (2020) (n 23).
[129] See fn 123 above.
[130] John Kennedy, 'Ireland is the data capital of Europe, says Google (video)' *SiliconRepublic* (4 February 2016). See also McIntyre (2015). For a critique of the high-tech narrative, see Martyn Egan, '"The Mystery of Dublin" – Corporate Profit-shifting and Housing Crisis in Twenty-first Century Ireland' (2023) *Political Economy*, https://doi.org/10.1080/03085147.2023.2187997.