Configuration Manual

The Impact of COVID-19 and the War in Ukraine on Cybersecurity in Small to Medium-Sized Law Firms in Ireland and the United Kingdom

Carlos Da Silva
Student ID: x22210113

School of Computing
National College of Ireland

Supervisor: Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Carlos Da Silva

Student ID: X22210113

Programme: MSc in Cybersecurity **Year:** 2024

Module: Masters

Supervisor: Raza Ul Mustafa

Submission Due Date: 15th September 2024

Project Title: The Impact of COVID-19 and the War in Ukraine on Cybersecurity in Small to Medium-Sized Law Firms in Ireland and the United Kingdom

Word Count: 4,017 **Page Count** 14

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Carlos Da Silva
Student ID: x22210113

1 Introduction

This configuration manual is designed to accompany my research paper, providing descriptions of the technical specifications and configurations used throughout my research. It is intended to guide other researchers, academic peers, and anyone interested in replicating or reviewing the technical aspects of my study. The manual outlines the hardware and software configurations, installation procedures, and operational guidelines.

2 Link to Video

3 Slides used for Video

Attached to this document, and sent separately.

4 Documents Structure

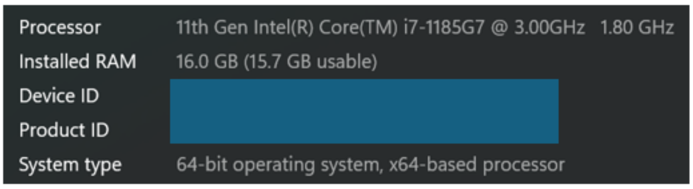
Sections 3 describes the hardware and software used as part of this research. Section 4 details the R Code used to analyse the survey results. Section 5 discusses the management of the data, including security considerations. The Appendix includes are supporting material such as questions sets etc.

5 System Specifications

For this project I used my personal laptop, a dual monitor set up, a proprietary operating system (OS) and paid and open-source applications.

5.1 Hardware

Dell Latitude 7420, i7 Processor and 16 gigabytes (GB) of random-access memory (RAM) - see Figure 1. Additional two monitor set up.



Processor	11th Gen Intel(R) Core(TM) i7-1185G7 @ 3.00GHz 1.80 GHz
Installed RAM	16.0 GB (15.7 GB usable)
Device ID	[redacted]
Product ID	[redacted]
System type	64-bit operating system, x64-based processor

Figure 1: Laptop specification.

5.2 Operating System

Licensed installation of Microsoft Windows 11 with 23H2 Service Pack.

5.3 Software

Paid Applications
Licensed installation of Microsoft Office, predominantly Word, Excel and PowerPoint. Microsoft Forms (online) was used to create the survey.

Open-Source Applications
Note: R Studio was installed with the intention of analysing the survey responses. However, I encountered numerous challenges as a result of the structure of the survey questions. Further research highlighted the correct structure required, but at that stage the surveys had been sent out to recipients. While every effort was made to get this to work correctly, I ended up using Excel to analyse the information required to complete the project. An example of the Excel process is provided below.

R version 4.41, and RStudio version 2024.04.2 Build 764 were installed using the following guide and links:

https://posit.co/download/rstudio-desktop/

https://rstudio-education.github.io/hopr/starting.html

http://rafalab.dfci.harvard.edu/dsbook/getting-started.html

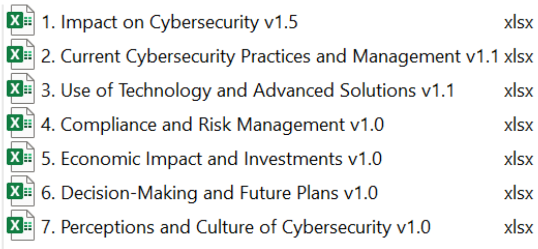
Firefox version 129.0 (64-bit) was installed and used as the default browser.

5.4 Installation and Setup

RStudio was installed for an earlier module in the course, and the decision was made to leverage the capabilities to analyse the data gathered from the survey.

5.5 Survey Analysis

The results of all the survey responses were collated into one master spreadsheet. The questions were then grouped according to the key research criteria. Once these groupings were established, a new spreadsheet was created for each grouping, as seen in Figure 2.

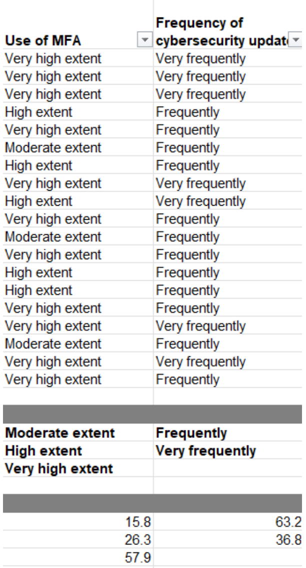


1. Impact on Cybersecurity v1.5	xlsx
2. Current Cybersecurity Practices and Management v1.1	xlsx
3. Use of Technology and Advanced Solutions v1.1	xlsx
4. Compliance and Risk Management v1.0	xlsx
5. Economic Impact and Investments v1.0	xlsx
6. Decision-Making and Future Plans v1.0	xlsx
7. Perceptions and Culture of Cybersecurity v1.0	xlsx

Figure 2: List of Survey Grouping Spreadsheets

This was carried out with the intention of using with R Studio, but the data was ultimately analysed using Excel. The structure of the survey did not lend itself to more complex analytical methods using R. This was ultimately due to inexperience with R and the way in which the survey was structured, rather than any deficiencies with the tool itself. For this reason, the analysis was carried out using Excel.

For example, for the section “Current Cybersecurity Practices and Management” the extracted data was cleaned up, any identifying columns were removed, and a summary for each response type was calculated below the respective column as a percentage. Figure 3 shows an extract of the survey analysis.

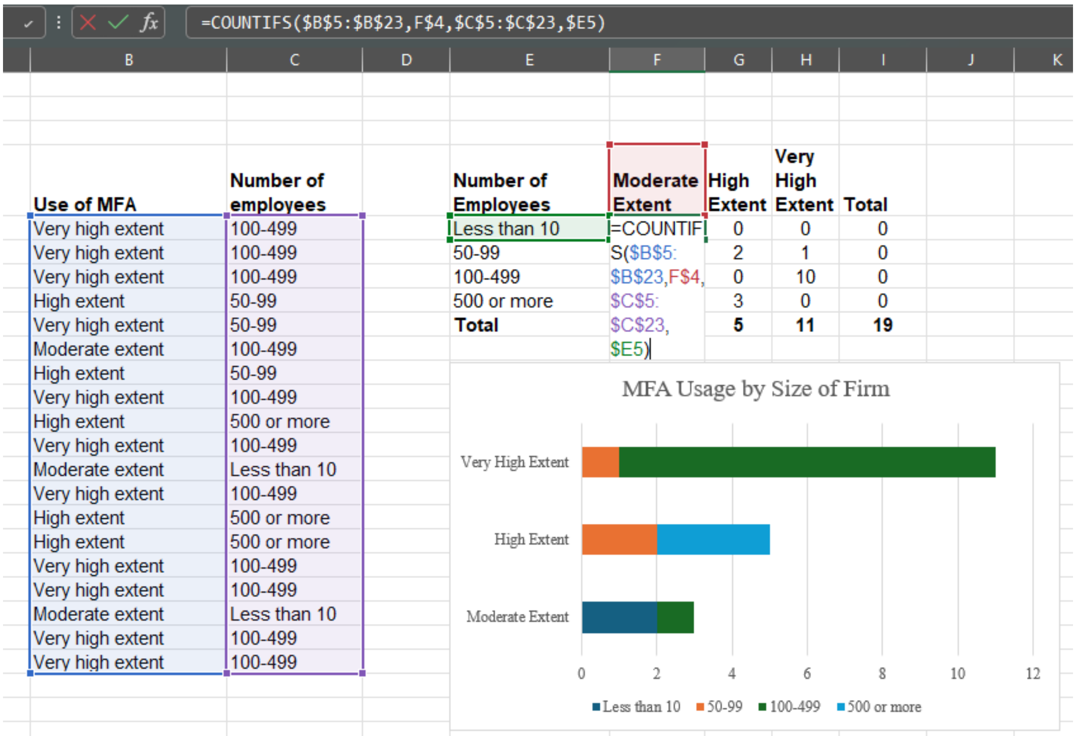


Use of MFA	Frequency of cybersecurity updat
Very high extent	Very frequently
Very high extent	Very frequently
Very high extent	Very frequently
High extent	Frequently
Very high extent	Frequently
Moderate extent	Frequently
High extent	Frequently
Very high extent	Very frequently
High extent	Very frequently
Very high extent	Frequently
Moderate extent	Frequently
Very high extent	Frequently
High extent	Frequently
High extent	Frequently
Very high extent	Frequently
Very high extent	Very frequently
Moderate extent	Frequently
Very high extent	Very frequently
Very high extent	Frequently
Moderate extent	**Frequently**
High extent	**Very frequently**
Very high extent	
15.8	63.2
26.3	36.8
57.9	

Figure 3: Extract of Survey Analysis

A set of helper rows were created to provide the percentage of each response. In each grouping spreadsheet, the firm’s size, years in operation and speciality were added. The revenue field was not used, as this may inadvertently identify a firm.

An analysis worksheet was created to carry out further analysis, such as determining the usage of a particular technology based on the size of the firm. A formula was used to calculate the total by firm size, and a graph was inserted based on this data. The formula can be seen in Figure 4.



```
=COUNTIFS($B$5:$B$23,F$4,$C$5:$C$23,$E5)
```

Use of MFA	Number of employees
Very high extent	100-499
Very high extent	100-499
Very high extent	100-499
High extent	50-99
Very high extent	50-99
Moderate extent	100-499
High extent	50-99
Very high extent	100-499
High extent	500 or more
Very high extent	100-499
Moderate extent	Less than 10
Very high extent	100-499
High extent	500 or more
High extent	500 or more
Very high extent	100-499
Very high extent	100-499
Moderate extent	Less than 10
Very high extent	100-499
Very high extent	100-499

Number of Employees	Moderate Extent	High Extent	Very High Extent	Total
Less than 10	=COUNTIFS($B$5:$B$23,F$4,$C$5:$C$23,$E5)	0	0	0
50-99		2	1	0
100-499		0	10	0
500 or more		3	0	0
Total		**5**	**11**	**19**

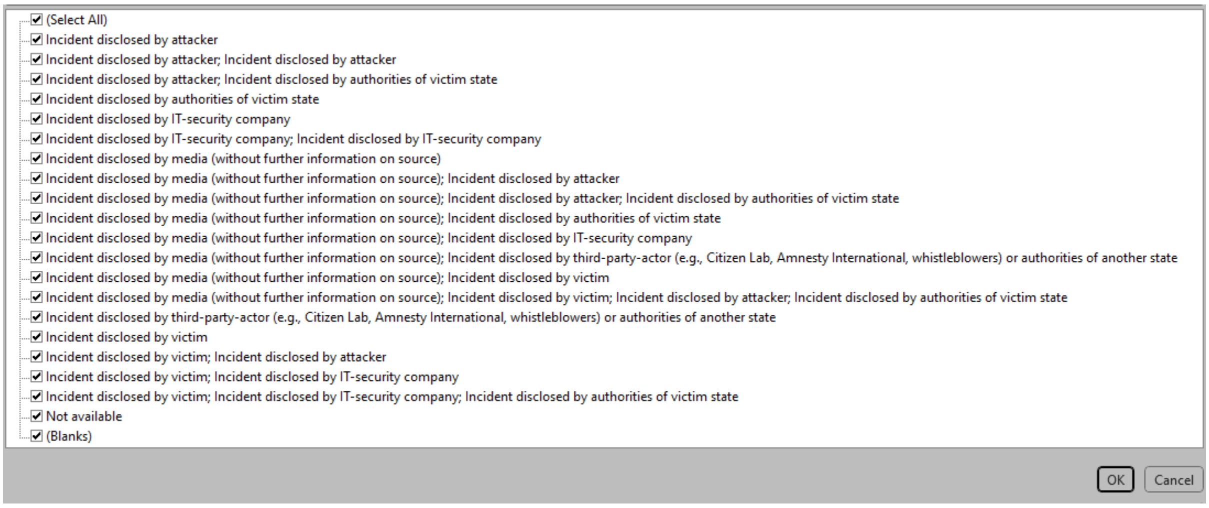
Figure 4: Sample of Analysis Worksheet Calculations

6 Data Management

Due consideration was given to ensuring the data was protected in transit and at rest. The publicly available data set was downloaded from EuRepoC and stored in an encrypted OneDrive folder. The survey data was downloaded to the same location.

6.1 EuRepoC Public Data Set

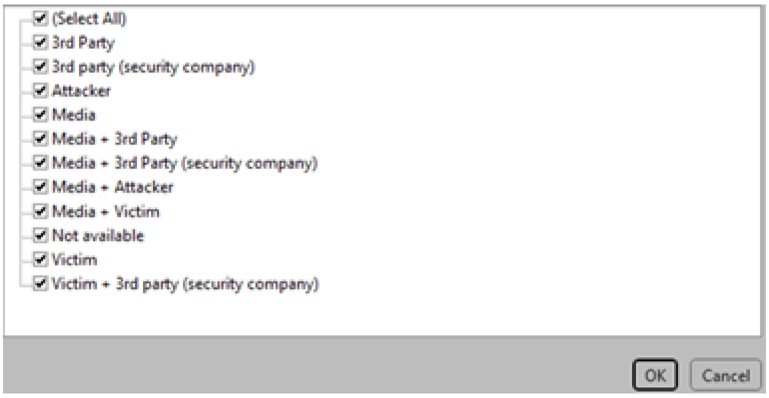
The public data set was filtered to contain only EU Region data from 2018 to 2024 inclusive. The data is provided by Heidelberg University in Germany. Permission is granted by the university to use the data set “for personal, scientific, or non-commercial uses” (Anon, n.d.). The data was downloaded in spreadsheet format and analysed using Microsoft Excel.
In order to work with the data, additional helper columns were added to streamline the data. For example, the method of disclosure had multiple criteria for classifying the source – see Figure 5.



☑ (Select All)
☑ Incident disclosed by attacker
☑ Incident disclosed by attacker; Incident disclosed by attacker
☑ Incident disclosed by attacker; Incident disclosed by authorities of victim state
☑ Incident disclosed by authorities of victim state
☑ Incident disclosed by IT-security company
☑ Incident disclosed by IT-security company; Incident disclosed by IT-security company
☑ Incident disclosed by media (without further information on source)
☑ Incident disclosed by media (without further information on source); Incident disclosed by attacker
☑ Incident disclosed by media (without further information on source); Incident disclosed by attacker; Incident disclosed by authorities of victim state
☑ Incident disclosed by media (without further information on source); Incident disclosed by authorities of victim state
☑ Incident disclosed by media (without further information on source); Incident disclosed by IT-security company
☑ Incident disclosed by media (without further information on source); Incident disclosed by third-party-actor (e.g., Citizen Lab, Amnesty International, whistleblowers) or authorities of another state
☑ Incident disclosed by media (without further information on source); Incident disclosed by victim
☑ Incident disclosed by media (without further information on source); Incident disclosed by victim; Incident disclosed by attacker; Incident disclosed by authorities of victim state
☑ Incident disclosed by third-party-actor (e.g., Citizen Lab, Amnesty International, whistleblowers) or authorities of another state
☑ Incident disclosed by victim
☑ Incident disclosed by victim; Incident disclosed by attacker
☑ Incident disclosed by victim; Incident disclosed by IT-security company
☑ Incident disclosed by victim; Incident disclosed by IT-security company; Incident disclosed by authorities of victim state
☑ Not available
☑ (Blanks)

Figure 5: Unfiltered Disclosure List.

A helper column was added to improve classification criteria and allow for better analysis. In this case, the first reporting entity was used as the key criteria – see Figure 6.



☑ (Select All)
☑ 3rd Party
☑ 3rd party (security company)
☑ Attacker
☑ Media
☑ Media + 3rd Party
☑ Media + 3rd Party (security company)
☑ Media + Attacker
☑ Media + Victim
☑ Not available
☑ Victim
☑ Victim + 3rd party (security company)

Figure 6: Helper Column with Refined Disclosure List.

A series of pivot tables were used to create the analyses of the public data set.

7 Appendices

Two sets of questions were compiled for the research paper. The first set covers the survey sent out via Microsoft Forms. The second set was compiled for the two case studies that were carried out.

7.1 Survey Email Template

Sample of the email template sent to target audience.

Subject: Request for Participation in Survey on the impact of Global Events on Cybersecurity in the Legal Sector

Hi [Recipient]

I hope this message finds you well. I am presently completing a Masters in Cybersecurity at National College of Ireland. I am currently conducting research for my dissertation on the impact of Covid-19 and the War in

Ukraine on Cybersecurity in the Legal Sector. As part of this study, I am seeking participants to complete a survey that will provide valuable insights into cybersecurity practices in the legal sector.

Your participation in this survey would be immensely valuable. By contributing, you will not only assist in advancing academic research but also gain access to the aggregated results of the survey. This will enable you to compare your firm's cybersecurity posture against current trends and benchmarks within similar firms. Understanding these trends can help you identify areas for improvement and implement more effective cybersecurity measures.

The survey will take approximately 15 minutes to complete. Your responses will be completely anonymous, and the data will be fully anonymised before being aggregated and analysed. No personally identifiable information, or information that can specifically identify your firm. will be collected or stored.
To participate, please follow this link to the survey: [Link]

Additionally, kindly reply to this email confirming your participation and consent to be part of the study.
By completing the survey, you are giving your consent to participate in this study. Participation is entirely voluntary, and you may withdraw at any time without any consequence.

If you have any questions or concerns about this research, please do not hesitate to contact me at x22210113@student.ncirl.ie.

Thank you very much for considering this request. Your input is crucial to the success of my research, and I greatly appreciate your time and contribution.

Best regards,
Carlos Da Silva
National College of Ireland
School of Computing
087 628 1001
x22210113@student.ncirl.ie

7.2 Survey Question Set

List of questions used for survey of law firms in Ireland and the UK.

Question Numbers	Question
1	ID
2	Start time
3	Completion time
4	Email
5	Name
6	Last modified time
7	Email Address (Optional)
8	How frequently has your firm experienced phishing attacks since the start of the COVID-19 pandemic in 2020?
9	How often has your firm encountered Distributed Denial of Service (DDoS) attacks in the last four years?
10	Do you consider your firm in scope for the threat of state-sponsored cyberattacks due to the geopolitical tension from the war in Ukraine?
11	In the last four years, how often did your firm receive emails or messages with COVID-19-related themes that you suspect were phishing attempts?

12	How adequately do you feel your firm's cybersecurity protocols protect against new threats?
13	To what extent does your firm employ multi-factor authentication for secure access?
14	How frequently does your firm update its cybersecurity software and systems?
15	How effective are your current cybersecurity incident response plans (CIRP)?
16	To what extent do you feel your firm's employees are trained in cybersecurity best practices?
17	How significantly did the transition to remote work during the pandemic impact your firm's cybersecurity?
18	How often did your firm use unsecured personal devices for work purposes during the pandemic?
19	To what extent did inadequate home network security pose a threat to your firm's cybersecurity during remote work?
20	How effectively did your firm manage the increased cyber threats during the pandemic?
21	How comprehensive was the cybersecurity guidance provided to employees during the pandemic?
22	How significantly has the war in Ukraine impacted your firm's cybersecurity measures?
23	To what extent do you believe geopolitical tensions have increased cyber threats to your firm?
24	How often have you noticed an increase in cyberattacks against your firm since the start of the war in Ukraine?
25	How effectively has your firm adapted its cybersecurity strategies in response to the war in Ukraine?
26	How well prepared do you feel your firm is for potential cyber threats related to geopolitical events?
27	To what extent does your firm use AI-driven cybersecurity solutions?
28	How effective do you find AI in detecting and responding to cyber threats?
29	How significantly do you believe AI can improve your firm's cybersecurity posture?
30	To what extent do you feel prepared to defend against AI-enhanced cyberattacks?
31	How frequently has your firm encountered deepfake scams using AI?
32	To what extent have cyber threats impacted your firm's operational efficiency?
33	How frequently does your firm invest in cybersecurity upgrades to mitigate economic losses?
34	How significant is the cost of recovering from cyberattacks for your firm?
35	How effective are your current investments in reducing the economic impact of cyber threats?
36	How well does your firm comply with the General Data Protection Regulation (GDPR)?
37	To what extent do you feel prepared to meet the requirements of the NIS2 Directive?
38	How frequently do you conduct security audits to ensure compliance with relevant regulations?
39	How significant are the legal implications of cyberattacks for your firm?
40	How effectively do your firm's cybersecurity measures help you comply with EU regulations?
41	How effective are your firm's current cybersecurity measures in mitigating risks?
42	To what extent has your firm adopted secure communication tools and virtual private networks (VPNs)?
43	How often do you review and update your cybersecurity policies?
44	How significant is employee training in your overall cybersecurity strategy?
45	How effectively do you collaborate with other firms or organisations to improve cybersecurity?
46	How confident are you in your firm's ability to handle future cyber threats?
47	To what extent does your firm plan to invest in new cybersecurity technologies in the next year (2025)?
48	Does your firm continuously monitor for cybersecurity threats?
49	How often does your firm carry out cybersecurity training and awareness programs?
50	How significant do you find the role of cybersecurity in maintaining client trust?
51	How prepared is your firm to adapt to new and emerging cybersecurity threats?
52	How effectively do you incorporate feedback from cybersecurity incidents into your future strategies?

53	To what extent does your firm use observability tools to monitor cybersecurity threats?
54	Does your firm use a Security Incident and Event Management (SIEM) platform?
55	Does your firm have a Security Operations Centre (SOC)?
56	How frequently do you review the data collected by your observability tools?
57	How comprehensive are the metrics and logs provided by your current observability tools?
58	To what extent do you use real-time monitoring solutions to detect cybersecurity incidents?
59	How confident are you that your firm's observability tools provide accurate and timely insights into potential threats?
60	To what extent do you believe your firm's current observability tools adequately identify all relevant cybersecurity threats?
61	How confident are you in your firm's ability to use observability tools to detect anomalous behaviour in your systems?
62	To what extent do your firm's observability tools help you proactively identify vulnerabilities?
63	How effective do you find your firm's observability tools in reducing the time to detect and respond to incidents?
64	In your opinion, does your firm's senior management understand the importance of investment in cybersecurity?
65	In your opinion, does your firm's senior management provide sufficient support for cybersecurity initiatives?
66	Is cybersecurity on the agenda for your firm's senior management?
67	How many employees does your firm have?
68	What is the primary area of specialisation for your law firm?
69	Is your law firm primarily located in the UK or Ireland?
70	(Optional) What is the annual revenue of your law firm?
71	How many years has your law firm been in operation?

7.3 Survey Question Groupings

1	**Impact of COVID-19 and War in Ukraine on Cybersecurity**
2	How frequently has your firm experienced phishing attacks since the start of the COVID-19 pandemic in 2020?
3	How often has your firm encountered Distributed Denial of Service (DDoS) attacks in the last four years?
4	Do you consider your firm in scope for the threat of state-sponsored cyberattacks due to the geopolitical tension from the war in Ukraine?
5	In the last four years, how often did your firm receive emails or messages with COVID-19-related themes that you suspect were phishing attempts?
11	How significantly did the transition to remote work during the pandemic impact your firm's cybersecurity?
12	How often did your firm use unsecured personal devices for work purposes during the pandemic?
13	To what extent did inadequate home network security pose a threat to your firm's cybersecurity during remote work?
14	How effectively did your firm manage the increased cyber threats during the pandemic?

15	How comprehensive was the cybersecurity guidance provided to employees during the pandemic?
16	How significantly has the war in Ukraine impacted your firm's cybersecurity measures?
17	To what extent do you believe geopolitical tensions have increased cyber threats to your firm?
18	How often have you noticed an increase in cyberattacks against your firm since the start of the war in Ukraine?
20	How well prepared do you feel your firm is for potential cyber threats related to geopolitical events?
19	How effectively has your firm adapted its cybersecurity strategies in response to the war in Ukraine?

2	**Current Cybersecurity Practices and Management**
6	How adequately do you feel your firm's cybersecurity protocols protect against new threats?
7	To what extent does your firm employ multi-factor authentication for secure access?
8	How frequently does your firm update its cybersecurity software and systems?
9	How effective are your current cybersecurity incident response plans (CIRP)?
10	To what extent do you feel your firm's employees are trained in cybersecurity best practices?
37	How often do you review and update your cybersecurity policies?
38	How significant is employee training in your overall cybersecurity strategy?
39	How effectively do you collaborate with other firms or organisations to improve cybersecurity?
36	To what extent has your firm adopted secure communication tools and virtual private networks (VPNs)?
40	How confident are you in your firm's ability to handle future cyber threats?

3	**Use of Technology and Advanced Solutions**
21	To what extent does your firm use AI-driven cybersecurity solutions?
22	How effective do you find AI in detecting and responding to cyber threats?
23	How significantly do you believe AI can improve your firm's cybersecurity posture?
24	To what extent do you feel prepared to defend against AI-enhanced cyberattacks?
25	How frequently has your firm encountered deepfake scams using AI?
47	To what extent does your firm use observability tools to monitor cybersecurity threats?

48	Does your firm use a Security Incident and Event Management (SIEM) platform?
49	Does your firm have a Security Operations Centre (SOC)?
50	How frequently do you review the data collected by your observability tools?
51	How comprehensive are the metrics and logs provided by your current observability tools?
52	To what extent do you use real-time monitoring solutions to detect cybersecurity incidents?
53	How confident are you that your firm's observability tools provide accurate and timely insights into potential threats?
54	To what extent do you believe your firm's current observability tools adequately identify all relevant cybersecurity threats?
55	How confident are you in your firm's ability to use observability tools to detect anomalous behaviour in your systems?
56	To what extent do your firm's observability tools help you proactively identify vulnerabilities?
57	How effective do you find your firm's observability tools in reducing the time to detect and respond to incidents?

4	**Compliance and Risk Management**
30	How well does your firm comply with the General Data Protection Regulation (GDPR)?
31	To what extent do you feel prepared to meet the requirements of the NIS2 Directive?
32	How frequently do you conduct security audits to ensure compliance with relevant regulations?
33	How significant are the legal implications of cyberattacks for your firm?
34	How effectively do your firm's cybersecurity measures help you comply with EU regulations?
35	How effective are your firm's current cybersecurity measures in mitigating risks?

5	**Economic Impact and Investments**
26	To what extent have cyber threats impacted your firm's operational efficiency?
27	How frequently does your firm invest in cybersecurity upgrades to mitigate economic losses?
28	How significant is the cost of recovering from cyberattacks for your firm?
29	How effective are your current investments in reducing the economic impact of cyber threats?

6	**Decision-Making and Future Plans**
44	How significant do you find the role of cybersecurity in maintaining client trust?

45	How prepared is your firm to adapt to new and emerging cybersecurity threats?
41	To what extent does your firm plan to invest in new cybersecurity technologies in the next year (2025)?
42	Does your firm continuously monitor for cybersecurity threats?
43	How often does your firm carry out cybersecurity training and awareness programs?
46	How effectively do you incorporate feedback from cybersecurity incidents into your future strategies?

7	**Perceptions and Culture of Cybersecurity**
58	In your opinion, does your firm's senior management understand the importance of investment in cybersecurity?
59	In your opinion, does your firm's senior management provide sufficient support for cybersecurity initiatives?
60	Is cybersecurity on the agenda for your firm's senior management?

7.4 Case Study Question Set

List of questions used for case studies carried out with two law firms in Ireland.

Background Information	
Have there been any major changes in your firm in the last six years?	

Current Cybersecurity Management	
How is your firm's cybersecurity currently managed (in-house, outsourced, or both)?	
What influenced your decision to manage cybersecurity in this manner?	
Would you consider changing this approach? If so, why?	
What measures (broadly) does your firm have in place to protect your legaltech solutions (case management etc.)? Do you feel these measures are adequate?	

Reasons for Outsourcing or Keeping In-house	
If you outsource your cybersecurity, what key factors influenced this decision?	
If managed in-house, what advantages do you perceive in this approach compared to outsourcing?	

Satisfaction with Current Cybersecurity Model	
How satisfied are you with your current cybersecurity management model?	
What improvements or changes would you consider to enhance the effectiveness of your cybersecurity strategy?	

Role of Cybersecurity in Operational Priorities	
How important is cybersecurity among your firm's operational priorities?	
Have these priorities shifted in the past few years, and if so, what prompted these changes?	
Have external factors such as COVID-19 or the war in Ukraine influenced your cybersecurity strategies? Please elaborate.	

Impact of Cybersecurity Management on Compliance and Risk	
How does your current cybersecurity approach impact your compliance with relevant regulations (e.g., GDPR, NIS2 Directive)?	
What effect has your chosen cybersecurity management model had on your risk profile?	
What preparations has your firm made to ensure compliance with the NIS2 Directive coming into effect in January 2025?	

Challenges with Current Cybersecurity Practices	
What are your most significant challenges with your current cybersecurity management approach?	
How do these challenges affect your operational effectiveness and security posture?	

Decision-Making Process for Cybersecurity Investments	
Who is responsible for making decisions about cybersecurity investments within your firm?	
How are these decisions influenced by the outcomes of your cybersecurity measures?	

Future Plans for Cybersecurity Management	
Are there any plans to change how your cybersecurity is managed in the near future?	
What factors might prompt a reconsideration of your current cybersecurity management model?	

Overview of Cybersecurity Evolution in the Firm	
How has your firm's approach to cybersecurity evolved over the past six years?	
What significant changes have been implemented in your cybersecurity strategies during this period?	

Consistency in Cybersecurity Measures	
Which aspects of your cybersecurity practices have remained consistent over the last six years, and why?	
How effective have these consistent strategies been in managing cyber threats?	

Employee Training and Engagement	
How has the approach to employee training in cybersecurity changed over the years?	
What feedback do you receive from employees regarding cybersecurity awareness and training programs?	

Incident Reporting and Proactive Measures	
How have your employees' behaviours toward reporting potential cybersecurity threats like phishing evolved?	
Which proactive security measures have been the most and least effective?	

Challenges and Areas for Improvement	
Based on your experiences, what are your firm's primary cybersecurity challenges?	
What areas in your cybersecurity practices do you believe need urgent improvement?	

Impact of Organisational Changes on Security	
For the firm that was acquired: How did the acquisition impact your cybersecurity operations and policies?	
For the firm that remained independent: How have you adapted your cybersecurity measures in response to evolving cyber threats?	

Future Cybersecurity Strategies	
Looking ahead, what changes or enhancements are planned for your cybersecurity strategies?	
How do you plan to address the identified areas needing improvement?	

Perceptions of Cybersecurity Culture	
How would you describe the culture surrounding cybersecurity within your firm?	
What steps are being taken to enhance this culture and ensure a high level of security awareness?	

References

Anon 'Legal Notice'. *EuRepoC: European Repository of Cyber Incidents*. Available [Online] at: https://eurepoc.eu/legal-notice/. [Last accessed 10 August 2024].