

# 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

MSc Research Project  
MSc in Cybersecurity

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:** 12<sup>th</sup> August 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:** 12,423 ..... **Page Count** 25 (excluding references)

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:** 15/09/2024.....

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

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

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

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# 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  
x22210113

## Abstract

This study investigates the cybersecurity challenges faced by small to medium-sized law firms in Ireland and the UK, particularly in light of recent global crises such as the COVID-19 pandemic and the war in Ukraine. Through a comprehensive survey and detailed case studies, the research identifies the current state of cybersecurity practices, the impact of these crises on cyber threats, and the effectiveness of existing mitigation strategies. Key findings from the study reveal a significant increase in phishing attacks. Remote working challenges were most effectively mitigated by the significant deployment of Multi-Factor Authentication (MFA) and Virtual Private Network (VPN) technologies, as well as increased staff training focused on cybersecurity practices for teleworkers. Strong adoption of advanced technologies such as Artificial Intelligence (AI) and Security Incident and Event Management (SIEM) platforms were noted, with 63% of firms surveyed citing moderate to high use of AI for cyber defence, and 58% utilising a SIEM platform. The study highlights the importance of tailored cybersecurity solutions for the legal sector, emphasising the need for continuous improvement and targeted support for smaller firms. Proposals for future research include the development of a cybersecurity maturity model, the exploration of emerging technologies, and the establishment of collaborative cyber defence networks.

**Keywords:** Cybersecurity, Law Firms, COVID-19 Pandemic, Ukraine War, Phishing Attacks, AI, SIEM, GDPR Compliance, NIS2 Directive, Cybersecurity Training, Cyber Threats, Legal Sector

## 1 Introduction

Critical to the administration of justice and commercial transactions, the legal sector increasingly relies on robust cybersecurity to protect sensitive client information and maintain operational integrity. This is particularly crucial for small to medium-sized law firms, which significantly contribute to legal services across Ireland and the UK. These firms, often less equipped than their larger counterparts, face immense pressure to safeguard their digital infrastructures.

The onset of the COVID-19 pandemic at the start of 2020 triggered a rapid shift towards digital workflows and remote operations, steering these firms into a new era of cybersecurity challenges. Law firms, along with most other organisations, had to deal with the swift adoption of remote work arrangements with limited time to plan or prepare appropriate cybersecurity measures. This sudden transition exposed vulnerabilities such as unsecured home networks, increased use of personal devices and reliance of remote communication platforms such as Zoom and Microsoft Teams. This shift was further complicated by geopolitical tensions arising from the war in Ukraine, which expanded the scope of cyber

threats and tested the resilience of cybersecurity measures under unprecedented conditions. The combined impact of these events has reshaped cybersecurity considerations, introducing complex challenges that demand a focused examination.

During the research process, it became clear that most of the available literature on law firm cybersecurity pre-dates the pandemic, focusing mainly on recommendations and frameworks rather than recent data. This thesis addresses this gap by presenting a survey of current cybersecurity practices in law firms, providing updated insights and concluding with actionable recommendations for enhancing cyber security practices in the context of these global events.

## 2 Research Question

Each objective is designed to contribute distinct insights that collectively respond to the overarching research question, comprehensively analysing how external pressures transform cybersecurity dynamics within the legal sector.

**Research Statement:** What is the impact of COVID-19 and the war in Ukraine on small to medium-sized law firms in Ireland and the United Kingdom, specifically in terms of cybersecurity?

### Objectives:

This research explores how recent significant global events—namely, the COVID-19 pandemic and the conflict in Ukraine—have shaped cybersecurity practices within the legal sector.

1. **Examine the Increase in Cyber Threats:** Assess how the proliferation of advanced cyber tools and the rise of Malware-as-a-Service (MaaS) have escalated cyber threats against law firms.
2. **Analyse Cybersecurity Challenges and Vulnerabilities:** Identify new vulnerabilities within law firms' cybersecurity frameworks that have emerged due to these advanced threats and increased tool availability.
3. **Evaluate Mitigation Strategies:** Evaluate how effectively law firms have adapted their cybersecurity measures in response to more accessible and sophisticated cyber threats.
4. **Explore the Role of Advanced Technologies:** Investigate how both defensive and offensive uses of artificial intelligence (AI) and other advanced technologies have been impacted by their increased availability in the cybersecurity field.
5. **Assess Economic Impact:** Determine the financial implications of these elevated cyber threats on law firms, considering both direct damages and the cost of enhanced cybersecurity measures.
6. **Understand Legal and Regulatory Implications:** Examine the legal challenges and regulatory compliance issues that law firms face as they navigate this new, more hostile cyber environment.

This research paper aims to comprehensively understand how law firms can better prepare for and respond to evolving cyber threats, fostering more robust and adaptive cybersecurity practices amidst global challenges. Additionally, it will offer actionable insights and strategic recommendations to help law firms enhance their cybersecurity resilience in an increasingly complex and hostile digital environment.

### 3 Related Works

The motivation for this study stems from a unique blend of professional experience and scholarly insights. Having collaborated with law firms, I have observed firsthand the distinct cybersecurity challenges they encounter. This perspective is supported by recent scholarly articles and reports, such as the UK's National Cyber Security Centre's "Cyber Threat Report: UK Legal Sector" and the European Parliament's analyses on cybersecurity. These sources emphasise the urgency and relevance of addressing cybersecurity issues in the legal profession.

This research seeks to evaluate the impact of the COVID-19 pandemic and the war in Ukraine on law firms' cybersecurity practices and experiences in Ireland and the UK. It scrutinises the escalation of cyber threats, dissects vulnerabilities, and assesses mitigation strategies, particularly highlighting the role of advanced technologies like AI. This study gathers qualitative and quantitative data to develop a detailed understanding of these challenges and to propose actionable strategies for strengthening cybersecurity resilience via a survey-based methodology. The research aims to enrich the broader discourse on cybersecurity within the legal sector through this comprehensive approach.

The literature review sets a foundation for understanding how recent global crises have increased international cyber risks, exposing deficiencies and opportunities within current mitigation strategies. This analysis establishes a context for investigating the current cybersecurity conditions affecting small to medium-sized law firms in Ireland and the UK, particularly in relation to these global events. The research seeks to identify emerging challenges and vulnerabilities, assess the effectiveness of existing defensive measures, and determine how advanced technologies can bolster cybersecurity resilience. Through this comprehensive examination, the study aims to provide valuable insights and practical recommendations to improve cybersecurity practices within the legal sector.

#### 3.1 Pre-2020 Perspective

A 2019 article published in the *Journal of Internet Law* (Moore, 2019) highlighted the importance of safeguarding legal information against cyber threats. It emphasised a holistic approach to cybersecurity across in-house legal teams and external parties with access to their data. Central to Moore's argument was cultivating a proactive cybersecurity culture within law firms. This culture change must be driven by senior management and seamlessly integrated into daily operations. Leadership should develop and actively enforce information security policies and procedures, embedding cybersecurity as a top organisational priority. Common to both was the recommendation to implement a business continuity plan (BCP) to minimise disruption and conduct regular security risk and compliance assessments. These assessments are pivotal in identifying and mitigating potential cybersecurity risks, ensuring firms align with industry standards and regulatory requirements, and proactively addressing threats.

In the event of a data breach, Moore advocated for a documented cyber incident response plan (CIRP). This plan should delineate specific roles and responsibilities, monitoring and detection procedures, personnel training, containment steps, reporting policies, and mechanisms for notifying affected parties. The framework stressed the need for comprehensive technical and physical safeguards. Technical measures include IT security management, vulnerability testing, data encryption, and secure information disposal. Physical

safeguards must be implemented to protect against unauthorised access and ensure the secure disposal of confidential documents.

Legal firms often rely on technology specific to their needs, known as legaltech. This term refers to technology and software used to provide legal services and support operations within the legal industry. These sector specific technologies are increasingly crossing borders through suppliers and expanding consumer-facing services like LegalZoom and RocketLawyer (Rocket Lawyer and ELS Bringing Affordable Legal Service to Europe, n.d.). Despite these developments, the sector remains proportionally small, and investment in legaltech businesses, while growing, is overshadowed by investment in other industries. A research paper commissioned in 2019 by the Legal Services Board (LSB) (Hook & Tangaza, n.d.) investigates the impact of technology on the global legal sector, with a significant focus on cybersecurity. The study reveals that this economy is relatively small despite notable growth compared to sectors like financial services. It also highlights the diversity and scope of technological activities within the legal field worldwide, noting that many solutions aim to improve efficiency within law firms and corporate legal departments. However, the critical importance of considering cybersecurity when adopting these technologies is also emphasised.

The study finds that legal technology is beginning to significantly impact consumer legal services through platforms offering legal advice and DIY legal solutions. Trends like the rise of lawyer and legal advice platforms, services addressing unmet legal needs, and online dispute resolution (ODR) services are becoming more common. These advancements require robust cybersecurity measures to protect sensitive client information from escalating cyber threats in an increasingly connected and digital world.

The report identifies varied approaches by legal regulators worldwide, ranging from resistance to active facilitation of legaltech. Most regulators are cautious, often viewing legaltech as a professional competence issue rather than a regulatory one. By drawing parallels with other industries like financial services, healthcare, and automotive, the paper emphasises the importance of regulatory sandboxes, cross-border cooperation, and adapting regulatory frameworks to new business models, especially cybersecurity.

Legal regulators face significant challenges, including the need to rethink traditional regulatory models, manage the impact of AI, and address the growing disparity between B2B (Business to Business) and B2C (Business to Consumer) legaltech markets. The risk of inaction is highlighted, suggesting it could hinder the development and adoption of beneficial technologies while exacerbating cybersecurity vulnerabilities.

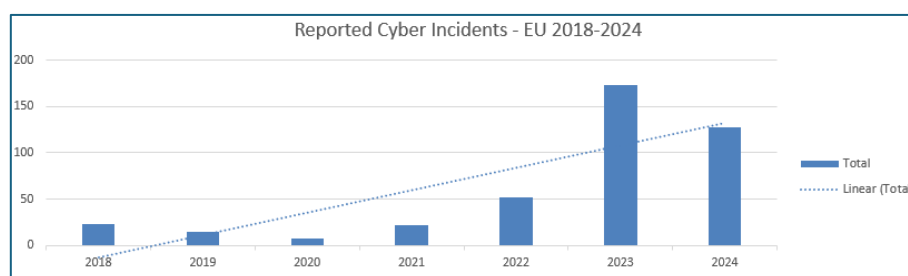
The paper stresses the need for strategic coordination, advisory panels, cross-border discussions, research into AI, the development of technology toolkits for entrepreneurs, and the establishment of minimum cybersecurity standards.

In conclusion, the paper underscores the necessity for legal regulators to adapt to the rapid advancements in legal technology, with a strong emphasis on cybersecurity. It advocates for a proactive approach, drawing lessons from other sectors to ensure that regulatory frameworks evolve alongside technological developments. The goal is to enhance the legal sector's efficiency, accessibility, and responsiveness to consumer needs while maintaining high cybersecurity standards, professional conduct, and public trust. Despite these insights, further work is required to fully understand how firms in different sectors, and sizes, have addressed these challenges. Barriers to entry such as internal resources, access to funding, and cost of legaltech services remain unclear. A broader, detailed international study would provide additional insight

## 3.2 Cyber Incident Reporting Trends

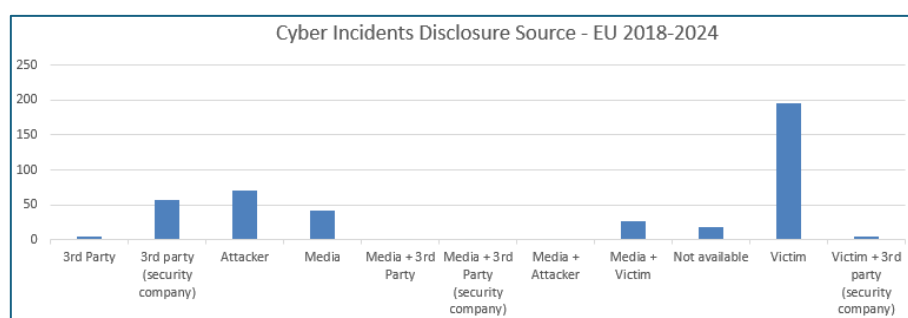
Data extracted from the EuRepoC public dataset (*Dashboard - EuRepoC: European Repository of Cyber Incidents*, n.d.) provides insights into cyber incident trends from 2000 to 2024. EuRepoC (European Repository of Cybers Incidents) is "an independent research consortium dedicated to better understanding the cyber threat environment in the European Union and beyond". EuRepoC has promoted data-driven discussions and policymaking within cybersecurity and raised awareness of cybersecurity threats. They achieve this by providing an analytical framework for assessing and comparing the 'lifecycle' of cyber incidents, focusing on technical, political, and legal aspects. Although this research paper focuses on Ireland and the UK, the extracted EuRepoC dataset's comprehensive coverage of the EU region provides a broader context for understanding regional cyber threats and trends.

As demonstrated in Figure 1, between 2018 to 2024 there has been a steady increase in reported cyber incidents. With regulations increasingly requiring victims of cyber incidents to report incidents to supervisory authorities, this is expected to increase (Aleksiev, 2023).



**Figure 1: Reported Cyber Incidents – EU 2018 to 2024.**

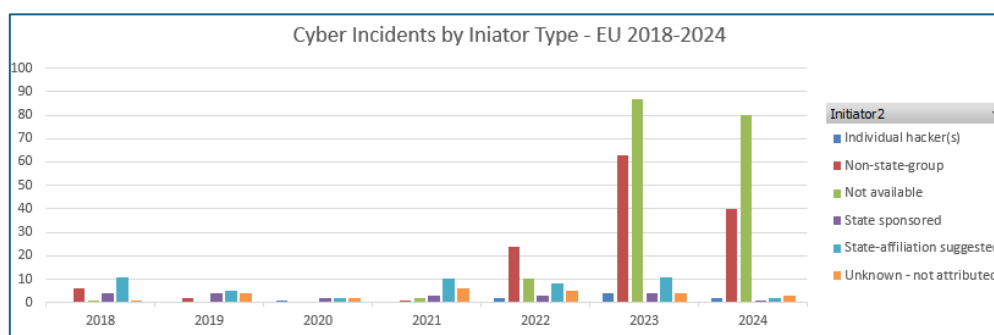
The data set also captured the varied sources of the reported incidents, with 17% being reported by the attacker, illustrated in Figure 2. This tactic is most likely used to apply pressure to the victim to coerce a ransom payment.



**Figure 2: Cyber Incident Disclosure by Source– EU 2018 to 2024.**

The data set shows the marked increase year-on-year in non-state-sponsored cyber attackers, contrasted with the slower rate of increase in state-sponsored attacks. Figure 3 highlights the significant rise in non-state-sponsored attacks, which may reflect a broader democratisation of cyber capabilities, where sophisticated tools and techniques have become more accessible to individual hackers and smaller groups. This shift in the threat landscape demands a re-evaluation of current cybersecurity policies and regulations. Policymakers are developing flexible and adaptive frameworks capable of addressing the rapid changes in cyber threat

tactics and the expanding array of actors. Furthermore, enhanced collaboration and intelligence sharing between the public and private sectors, as well as within international communities, are crucial. This cooperation should focus on rapidly disseminating information about emerging threats, particularly those posed by non-state sources, to strengthen collective defence mechanisms. This culture (and regulatory obligation) to share data will allow organisations in similar sectors to take proactive actions such as blocking malicious IP addresses and phishing domains. A good example of this in action can be seen in the Monetary Authority of Singapore's (MAS) information sharing platform for banking organisations (Cameron, 2023). Additionally, the increasing importance of investing in cutting-edge cybersecurity technologies, including AI-driven security solutions, must be considered. These technologies are essential for providing proactive defences and quicker responses to emerging threats, especially from non-state actors who might exploit novel or less predictable attack vectors.



**Figure 3: Cyber Incident Initiators by Type – EU 2018 to 2024.**

### 3.3 Impact of Covid-19 on EU Law Firms

A 2022 study by Professor Bronisław Sitek in Poland highlighted the significant disruptions experienced by law firms in the EU due to the COVID-19 pandemic (Sitek, 2022). The study revealed that many firms faced operational and economic challenges from lockdowns and court closures. According to a survey by the Supreme Bar Council, 87% of law firms saw revenue declines, with 45% reporting a decrease of over 50% during the height of the pandemic. At the same time, firms incurred increased expenses for ICT tools and employee training to facilitate remote work. However, the pandemic also accelerated the adoption of digital technologies and remote work practices, improving flexibility and efficiency. Legislative changes allowed for e-hearings, ensuring some continuity in legal services despite the restrictions. Despite difficulties with court procedures and financial strain, the forced adaptation to new technologies has positioned well-equipped law firms for better performance in the post-pandemic period. The increased use of ICT tools and digitisation of services over this time has made firms more resilient, potentially enhancing their future economic stability and operational effectiveness.

### 3.4 Increase in Cyber Threats Due to COVID-19 and the War in Ukraine

#### Cyber Threats During the COVID-19 Pandemic

The 2020 COVID-19 pandemic and the war in Ukraine, which began in 2022, significantly increased cyber threats, presenting unique challenges to organisations globally. The pandemic introduced several unique cybersecurity threats, particularly in the realm of phishing attacks.



One study (Abroshan et al., 2021; Hoheisel et al., 2023) that analysed over 1,100 targeted domains identified that phishing emails quadrupled during this period. Many of the attacks leveraged COVID-19-related themes to exploit the fear, anxiety, and stress caused by the pandemic. The rapid shift to remote work environments exposed new vulnerabilities, as employees often used personal devices and unsecured networks, increasing their susceptibility to cyberattacks (The Bucharest University of Economic Studies, Bucharest, Romania. et al., 2021). Additionally, cybercriminals diversified their techniques, employing not only traditional email phishing but also vishing (voice phishing), smishing (SMS phishing), and spear phishing (targeted phishing), often impersonating well-known brands to deceive victims (Jafar et al., 2022).

The pandemic heightened cyber threats due to the widespread adoption of remote work, while the war led to an increase in state-sponsored attacks (Saalman et al., 2023; Teichmann & Boticiu, 2023). Cybercriminals exploited the surge in remote work applications and the use of unsecured personal devices and home networks, heightening the risk of cybercrime victimisation (Ncubukezi, 2020; Tam et al., 2020; Van De Weijer et al., 2024). Many employees received minimal guidance on secure remote work, while IT staff were primarily focused on remote working enablement. Law firms faced significant cybersecurity challenges due to the rapid implementation of remote working and limited resources. Along with the increase in phishing attacks, the pandemic also saw a rise in the numbers and frequency of ransomware and Distributed Denial of Service (DDoS) attacks, exploiting vulnerabilities and fears related to COVID-19 (Abroshan et al., 2021; Hoheisel et al., 2023).

These threats highlight the critical need for enhanced cybersecurity measures and comprehensive user education to mitigate the risks associated with phishing and other cyber threats during such crises.

### **Cyber-Attacks Due to the War in Ukraine**

The war in Ukraine has significantly impacted global cybersecurity, introducing a complex assortment of cyber tools and threat actors that have reshaped the security environment. Russian cyberattacks, which have been ongoing since the annexation of Crimea in 2014, intensified with the 2022 invasion, targeting critical infrastructure such as public services, energy, media, and financial sectors in Ukraine (Duneva, 2023). These attacks have included traditional techniques like phishing and DDoS attacks, as well as more advanced methods such as data-wiping malware and AI deepfake technologies. This evolution in tactics has led to significant disruptions in essential services and extensive data theft (Duneva, 2023). The conflict has also seen the rise of cyber proxies, such as Ukraine's IT army, which has engaged in cyber operations against Russian assets, highlighting the blurred lines between state and non-state actors in cyber warfare (Jakobsson & Nielsen, 2023). Additionally, the crossover between cybercrime and cyberwarfare has become more pronounced, with Russian-based groups like the Conti Group and Killnet aligning with state interests and employing ransomware and wipers for strategic objectives (Gabrian, 2022; Saalman et al., 2023). This evolving threat environment has prompted international responses, including EU, American, and NATO initiatives to bolster cyber defences and protect critical infrastructure (Duneva, 2023). The persistent and adaptive nature of these cyber threats underscores the need for robust cybersecurity measures and international cooperation to mitigate the risks posed by such hybrid warfare tactics (Brantly & Brantly, 2024; Štruel, 2022).

The war in Ukraine escalated cyber-attacks on law firms, increasing cybersecurity risks and requiring enhanced measures to protect sensitive data (Saalman et al., 2023; Somogyi & Nagy, 2023). Collaboration between cybercriminal groups and state actors facilitated

sophisticated and coordinated attacks, particularly through Advanced Persistent Threats (APTs) and Ransomware-as-a-Service (RaaS) models (Gabrian, 2022). RaaS has enabled less skilled criminals to launch impactful attacks, exemplified by incidents like the DarkSide ransomware attack on the Colonial Pipeline (Saalman et al., 2023; Zhuravka et al., 2022).

### **Challenges and Policy Recommendations**

One study found that law firms struggled to adapt their cybersecurity strategies amid increased risks, requiring rapid adjustments and continuous monitoring (Somogyi & Nagy, 2023; Teichmann & Boticiu, 2023). Governments and organisations provided policy recommendations and support, including grants and training programs (Tam et al., 2020). The EU emphasised adopting the Network and Information Security Directive (NIS), along with the Cyber Resilience Act, to enhance cybersecurity frameworks (NIS Directive, n.d.; Tasheva, 2021). An updated version of NIS, called NIS2 comes into effect in October 2024.

### **Impact and Mitigation of Cyber Threats**

To address these evolving threats, law firms implemented several mitigation measures. Wider deployments of controls such as multi-factor authentication (MFA) and regular cybersecurity updates were crucial in mitigating risks. Employee training on cybersecurity best practices also played a significant role (Huaman et al., 2021; Teichmann et al., 2022). Additionally, law firms developed and tested incident response plans and invested in secure communication tools and virtual private networks (VPNs) to protect data transmitted over the internet. Despite these measures, continuous improvements are necessary to effectively address the evolving cyber threat challenges (Huaman et al., 2021; Teichmann et al., 2022).

## **3.5 Economic Impact on Law Firms**

**Increase in Cybercrime:** The rise in AI-enhanced cybercrime, exacerbated by the COVID-19 pandemic and the war in Ukraine, has had a significant economic impact on small and medium-sized law firms. Cyberattacks can lead to financial losses, reputational damage, and operational disruptions. A data breach is estimated to cost around \$8.19 million on average in the United States, and the annual effect on the global economy from cyberattacks is approximately \$400 billion (Guembe et al., 2022). Law firms are particularly vulnerable to cyberattacks due to their limited resources and often inadequate cybersecurity measures. These financial impacts are compounded by the costs associated with recovering from attacks, including legal fees, regulatory fines, and loss of client trust.

**Investment and Funding for Enhanced Cybersecurity:** Law firms need to invest in advanced cybersecurity measures to combat the increasing threat of AI-enhanced cybercrime. This includes adopting AI-driven security solutions, training employees on cybersecurity best practices, and implementing robust security policies. The investment required for enhanced cybersecurity measures can be substantial, but it is necessary to protect against the growing threat of cybercrime (Ali et al., 2023). Despite the high initial costs, investing in cybersecurity can save law firms money in the long run by preventing costly breaches and minimising downtime caused by cyberattacks.

## **3.6 Legal and Regulatory Implications for Law Firms in the EU**

In the last three years, there have been significant legal and regulatory developments in the EU aimed at enhancing cybersecurity and protecting businesses from cybercrime. Since

2018, the General Data Protection Regulation (GDPR) has set stringent requirements for data protection and privacy, and non-compliance can result in hefty fines. Additionally, the EU has introduced the Digital Services Act (DSA) and the Digital Markets Act (DMA) to regulate digital services and ensure a safer online environment (Hussin & Salwa Prilia Ginano, 2023) as well as the NIS2 directive. NIS2 has been introduced as an upgrade to the original Network and Information Systems (NIS) Directive, broadening the scope to include a wider array of entities under its mandate. This directive imposes stricter cybersecurity requirements on essential and important entities, requiring robust risk management practices and incident reporting to national authorities. NIS2 aims to enhance the resilience of network and information systems across the EU, promoting a more secure digital environment by addressing supply chain security and encouraging a collaborative information-sharing culture.

Law firms in the EU must comply with these regulations to avoid legal repercussions and protect their clients' data. Compliance requires implementing robust data protection measures, conducting regular security audits, and ensuring transparency in data handling practices. Failure to comply with these regulations can result in significant financial penalties and reputational damage (Hussin & Salwa Prilia Ginano, 2023).

Along with technical controls, practical cybersecurity training for all employees, including management, is vital to preventing data breaches caused by human error. Training programs should provide detailed instructions for incident response and include practical exercises, such as phishing simulations, to reinforce secure practices.

Moore (Moore, 2019) highlighted the risks associated with third parties having access to confidential information. Firms must ensure that vendors and service providers adhere to stringent security practices through thorough assessments, formal agreements, and continuous compliance monitoring.

Finally, Moore underscored the importance of staying informed about data protection regulations across different jurisdictions. Legal departments must proactively advise on the implications of these regulations to ensure comprehensive cybersecurity compliance and reduce the risk of data breaches.

This timely paper summarised best practice concepts that would resonate in subsequent years with the advent of COVID-19 and the war in Ukraine. As cyber threats continue to evolve, Moore's insights and recommendations remain highly relevant, offering a comprehensive blueprint for law firms aiming to protect sensitive legal information.

### **3.7 Overview of As-a-Service (AAS) Offerings and Roles in the Cybercrime Ecosystem**

The emergence of "as-a-service" (AAS) offerings in cybercrime has significantly altered cyber threats, making sophisticated tools and tactics accessible to a broader range of individuals and groups. These services provide necessary tools and foster a specialised ecosystem supporting their operation and distribution.

#### **Types of As-a-Service Offerings:**

**Ransomware-as-a-Service (RaaS):** This service allows individuals to lease or purchase ransomware tools, enabling attacks without extensive technical knowledge. Offered through darknet marketplaces, RaaS simplifies participation in ransomware campaigns and often includes support desk services for victims, with providers typically taking a percentage of the ransom as their fee (Alwashali et al., 2021; Meland et al., 2020).

**Malware-as-a-Service (MaaS):** MaaS makes advanced malware accessible to those with minimal technical skills. This service supports various roles, from development to distribution, enhancing the reach and effectiveness of malware (Davidson, 2021; Karo-Karo et al., 2023; Patsakis et al., 2024).

**Cybercrime-as-a-Service (CaaS):** CaaS provides a wide array of digital resources, including malware, botnets, hacking expertise, and databases of stolen information. It promotes specialisation among providers and facilitates sophisticated cyberattacks (Maestre Vidal et al., 2019; Mathew, 2023; Singh & Rahman, 2023).

**Obfuscation-as-a-Service:** This service helps malware developers disguise their code to evade antivirus detection, which is crucial for sustaining operations by reducing detection rates (Sembera et al., 2021).

**Impersonation-as-a-Service (IMPaaS):** IMPaaS offers comprehensive user profiles to facilitate large-scale user impersonation, helping attackers bypass multi-factor authentication systems through systematic profile collection and enforcement (Campobasso & Allodi, 2020).

These structured AAS offerings significantly enhance the effectiveness, reach, and resilience of cybercriminal activities. They underscore the commoditisation of cybercrime, making sophisticated cyberattacks more accessible and scalable, thereby creating a robust underground economy centred around digital attacks and cybercrime.

### 3.8 Offensive Security Tools and Malware Detection

Cybersecurity has been significantly influenced by the emergence and widespread use of offensive security tools (OSTs) and advancements in malware detection techniques. Originally intended to assist security researchers and defenders, these tools have evolved into dual-purpose arsenals, beneficial for defence but exploited by malicious actors for cyberattacks.

Several high-profile data breaches at organisations such as the National Security Agency (NSA) have led to the public disclosure of proprietary tools used for national security (Biddle, 2016). A significant breach by the Shadow Brokers (Schneider, n.d.) exposed critical weaknesses in the NSA's cybersecurity protocols, making top-secret tools, including zero-day exploits, publicly available. Many of these tools remain accessible online today, and while patches have been developed for most exploits, some systems remain vulnerable. The GitHub repository shown in Figure 4 contains the necessary files for executing an EternalBlue exploit.

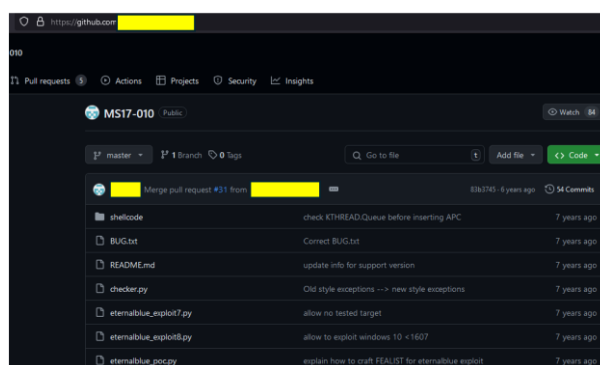
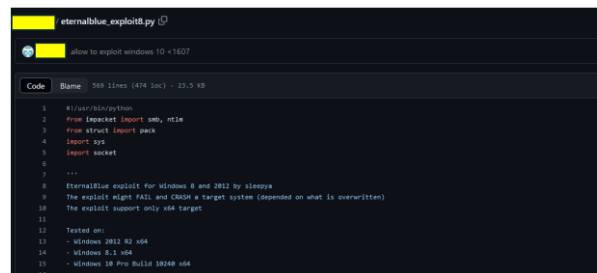


Figure 4: EternalBlue Exploit on GitHub.

Figure 5 displays an extract of the Python code from the EternalBlue exploit.



```
eternalblue_exploit.py
allow to exploit windows 10 +1607

Code 509 lines (1474 B) · 23.5 KB

1 #!/usr/bin/python
2 from struct import pack, unpack
3 from socket import socket
4 import sys
5
6 """
7
8 EternalBlue exploit for Windows 8 and 2012 by sleepys
9 The exploit might fail and CRASH a target system (depends on what is overwritten)
10 The exploit supports only x64 targets
11
12 Tested on:
13 - Windows 2012 R2 x64
14 - Windows 8.1 x64
15 - Windows 10 Pro Build 10240 x64
16 """
```

**Figure 5: EternalBlue Exploit Code.**

This breach compromised national security and facilitated the dissemination of advanced hacking tools to the public domain (*The “Shadow Brokers” NSA Theft Puts the Snowden Leaks to Shame*, 2016). These tools, initially designed for national security purposes, have since been repurposed for cybercrime, enabling the rise of Malware-as-a-Service (MaaS) platforms. The commoditisation of hacking tools through MaaS has significantly lowered the barrier to entry for cybercriminals, allowing individuals with minimal technical expertise to launch sophisticated cyber-attacks. This has fuelled the growing sophistication of cyber-attacks and highlighted the necessity for continuous improvements in corporate security measures.

This phenomenon illustrates a broader trend where the line between state-sponsored cyber espionage and organised cybercrime is increasingly blurred, posing severe risks to both national and corporate security.

Open-source tools (OSTs) like Mimikatz and UACME, originally developed for vulnerability assessment, have been co-opted by threat actors for malicious purposes, with adaptations of these tools found in numerous malware instances (*What Is Mimikatz?*, n.d.). Misusing code-signing Public Key Infrastructure (PKI) to disguise malware as trustworthy binaries poses a considerable security risk, emphasising the need for enhanced protective measures (Kim et al., 2017). Commercial tools such as Cobalt Strike, although intended for legitimate penetration testing, are frequently employed by cyber criminals and state-sponsored actors, blurring the lines between legitimate and malicious usage (Shaikhanoova & Kadyrov, 2023). State-sponsored malware like Stuxnet and Duqu have significantly disrupted global infrastructures (Bencs  th et al., 2012; Wangen, 2015). Proactive cyber threat intelligence and advanced malware detection methods, including machine learning and behavioural analysis, are essential (Samtani et al., 2017; Talukder & Talukder, 2020). The complex challenges presented by both OSTs and state-sponsored tools demand ongoing research and collaborative efforts within the cybersecurity community to develop robust mitigation strategies.

### 3.9 Role of Artificial Intelligence in Cybersecurity and Cybercrime

**Contribution to Cybersecurity:** AI has significantly enhanced the capabilities of cybersecurity systems by enabling more advanced and efficient threat detection and response. AI-powered systems can analyse vast amounts of data to identify patterns and anomalies that would be difficult or impossible for humans to detect. These systems can also respond to threats in real time, thereby improving the efficiency and effectiveness of cybersecurity measures (Shanthi et al., 2023) (Ali et al., 2023). By automating many aspects of

cybersecurity, AI helps law firms better manage their security operations and respond more quickly to incidents.

**Contribution to Cybercrime:** Conversely, cybercriminals have also exploited AI to carry out more sophisticated and effective attacks. AI enables the automation of various stages of cyberattacks, including reconnaissance, intrusion, privilege escalation, and data exfiltration. This automation allows cyber gangs to carry out attacks at a scale and speed that outpaces human-centred defence mechanisms (Chomiak-Orsa et al., 2019). AI-driven automation can generate automated payloads and conduct social engineering attacks, such as custom-made phishing, with minimal human intervention (Malatji, 2023). This increased sophistication of cyber-attacks makes it more challenging for law firms to protect themselves.

### 3.10 Recommendations and Strategies for Law Firms

Based on available research, the following table contains best practice recommendations for improving cybersecurity posture in small to medium size law firms.

<b>Implement AI-Driven Security Solutions:</b>	Law firms should invest in AI-driven security solutions that can provide real-time threat detection and response. These solutions can help identify and mitigate threats more efficiently and reduce the risk of cyberattacks (Shanthi et al., 2023).
<b>Employee Training and Awareness:</b>	Training employees on cybersecurity best practices is crucial for preventing cyberattacks. Law firms should conduct regular training sessions to educate employees about the latest threats and how to recognise and respond to them (Ali et al., 2023).
<b>Regular Security Audits:</b>	Regular security audits can help law firms identify system vulnerabilities and take corrective actions. These audits should include penetration testing, vulnerability assessments, and compliance checks (Hussin & Salwa Prilia Ginano, 2023).
<b>Data Protection Measures:</b>	Implementing robust data protection measures, such as encryption, access controls, and data backup, can help law firms protect their sensitive information from cyberattacks. These measures are essential for complying with data protection regulations and ensuring the security of client data (Hussin & Salwa Prilia Ginano, 2023).
<b>Collaboration and Information Sharing:</b>	Law firms should collaborate with other businesses, industry associations, and government agencies to share information about cyber threats and best practices. This collaboration can help law firms stay informed about the latest threats and improve their cybersecurity posture (Ali et al., 2023).

### **3.11 Summary**

The literature review establishes a comprehensive understanding of the increased cyber risks faced by law firms, particularly in the context of recent global crises like the COVID-19 pandemic and the war in Ukraine. Despite a robust body of existing research on cybersecurity across various industries, there remains a significant gap concerning the unique challenges encountered by small to medium-sized law firms. This gap is underscored by a general lack of specific data addressing these firms' particular vulnerabilities and requirements, which are often overlooked in favour of larger corporations. The reviewed literature reveals that while there are extensive insights into general cybersecurity practices, there is a critical need for focused research tailored to the legal sector's specific contexts and pressures.

This necessity justifies the research question that investigates the distinct cybersecurity challenges and the effectiveness of current mitigation strategies within law firms in Ireland and the UK. Given the escalation of non-state-sponsored cyber-attacks and the sophisticated use of technology by adversaries, as demonstrated in the literature, there is a compelling need to develop targeted strategies that enhance cybersecurity resilience specifically for the legal sector. This study seeks to fill the identified gaps by examining the current cybersecurity conditions, exploring emerging challenges, evaluating existing defences, and proposing actionable improvements. Such research is essential not only for enhancing the cybersecurity posture of law firms but also for contributing to the broader discourse on legal sector-specific cybersecurity solutions. While extensive research exists across various sectors a significant gap remains due to the lack of empirical studies on cybersecurity resilience in law firms since the start of the pandemic and the War in Ukraine.

## **4 Research Methodology**

This research investigates the impact of the COVID-19 pandemic and the war in Ukraine on the cybersecurity posture of small to medium-sized law firms in the Ireland and the UK using a quantitative survey method. The procedure involves survey design, distribution, data collection, anonymisation, and comprehensive reporting.

Surveys will be administered using Microsoft Forms, targeting law firms in Ireland and the UK. Stratified random sampling ensures diverse representation. Data was securely stored on cloud-based platform Microsoft OneDrive, and analysed using statistical software such as R, or Excel.

Key steps include defining research questions, developing a questionnaire on cybersecurity threats and measures, distributing the survey, and collecting responses. Data will be cleaned, anonymised, and analysed using descriptive and inferential statistics, including regression analysis to identify significant factors.

Results will be validated through multiple statistical techniques to ensure reliability. The final report will summarise findings, illustrate key data through visual aids, and provide actionable recommendations to enhance cybersecurity practices. This study aims to offer a detailed understanding of cybersecurity challenges and propose improvements for the law firms.

## **5 Design Specification**

The design of this study and the decision to use a survey-based methodology is driven by the need for comprehensive, quantifiable insights into the cybersecurity challenges faced by small to medium-sized law firms in Ireland and the UK. The survey employs a structured

questionnaire with a 1-5 Likert scale, followed by pilot testing to refine questions. Data is collected online through platforms like Microsoft Forms, encrypted during transmission and storage, and anonymised to protect respondent confidentiality. Analysis is carried out using R or Excel, applying descriptive and inferential statistics to summarise data and test hypotheses. Data is cleaned and standardised before analysis using descriptive and inferential statistics to ensure uniformity and reliability. The security framework incorporates encryption and anonymisation protocols.

The proposed Cybersecurity Threat Prioritisation Model (CTPM) aims to categorise and prioritise cybersecurity threats based on survey responses. The algorithm involves cleaning and normalising data, assigning weights to threats, and applying a ranking algorithm to generate a prioritised list of threats.

The structured approach ensures a rigorous examination of cybersecurity challenges, providing insights and actionable recommendations for small to medium-sized law firms in Ireland and the UK. Additional details available in the Configuration Manual which accompanies this paper.

## **6 Implementation**

In the final stage of the implementation, the survey data collected from small to medium-sized law firms was transformed and analysed. The output included comprehensive datasets detailing the cybersecurity practices, challenges, and effectiveness of various measures within these firms. Models were developed to identify key factors influencing cybersecurity resilience, and the Cybersecurity Threat Prioritisation Model (CTPM) was applied to categorise and rank threats based on the survey responses. The data analysis and model development were conducted using Excel. The survey questionnaires were also administered via Microsoft Forms. The final outputs provided actionable insights and recommendations to enhance the cybersecurity posture of the surveyed law firms.

## **7 Evaluation**

Two case studies were conducted, along with the survey.

### **7.1 Case Study 1**

This case study examines a mid-sized law firm in Ireland, focusing on the changes in its cybersecurity practices over the past six years. A key factor was the merger with a larger, global firm, which brought increased investment in cybersecurity tools, along with a more structured approach to compliance.

The firm's cybersecurity is managed using a hybrid model that combines in-house and outsourced resources, prioritising cost efficiency and governance control. The in-house team handles ticket incident and event management, cyber awareness activities, and trend monitoring, while specific tasks requiring specialised skills, such as log analysis, are outsourced to external experts for cost-effectiveness. This reliance on external specialist resources could potentially result in a knowledge gap within the firm's internal teams.



Even before COVID-19 and the war in Ukraine, the firm was already focused on strengthening its cybersecurity measures. However, these global events served as further catalysts, reinforcing the firm's approach in this area.

The COVID-19 pandemic impacted the firm's cybersecurity strategy by making the integration of remote working as a standard practice essential. This required extending the security perimeter to include home offices and multi-factor authentication (MFA) for client devices used outside the office. Additionally, the Irish government's stance on the war in Ukraine heightened the firm's focus on potential cyber threats, incorporating these considerations into their security posture.

During this time, the firm has employed a multi-tiered security approach, including external support to combat spoofed domains, standard desktop and firewall security, and a SIEM system monitored by a dedicated team. These measures are considered adequate for protecting the firm's legaltech solutions, such as the case management systems. The current cybersecurity strategy supports compliance with regulations such as GDPR and prepares the firm for the upcoming NIS2 Directive. Cybersecurity measures are a crucial factor for the firm when bidding for new business and with existing clients. The firm's risk profile has improved, and its compliance capabilities have been strengthened as a result of the investment in cybersecurity measures.

User compliance presents a significant challenge, with issues arising from either avoidance of compliance or frustration with the requirements. This increases false positives, negatively impacting the cybersecurity team's capacity. Despite these challenges, the firm maintains a "security first" culture, emphasising security over convenience. Regular employee training, including phishing simulation tests, has evolved to more individualised sessions, improving awareness and reporting of potential cyber threats. Sustaining high levels of user vigilance over time can present a challenge.

The firm is focused on continuous improvement and plans to explore AI tools to enhance its security posture. While no major changes to the cybersecurity management model are anticipated, the firm remains open to adapting its approach in response to large-scale security incidents or emerging trends.

In summary, this case study illustrates the measures taken in response to the COVID-19 pandemic and the war in Ukraine. The merger proved to be a catalyst for change in IT, specifically in cybersecurity. The firm's current hybrid cybersecurity model, enhanced user training, and proactive security culture have improved its resilience against evolving cyber threats, ensuring compliance and operational effectiveness in a complex and dynamic environment. Firms adopting this model should ensure that processes are well documented, and that internal teams work closely with external suppliers to close any knowledge gaps. An increased understanding of the work being carried out will ensure internal stakeholders have the required knowledge to make tactical and strategic decisions.

## **7.2 Case Study 2**

This case study examines a mid-sized law firm in Ireland, highlighting its evolving approach to cybersecurity over the past six years.

The firm's cybersecurity is managed through in-house resources, an IT partner, and an external Security Operations Centre (SOC). This blended approach is driven by the need to maximise protection within budget constraints while ensuring the latest cybersecurity measures are in place. The firm is committed to ISO27001 certification and employs a layered perimeter defence strategy, including daily alerting and proactive controls. Budget

constraints may limit the firm's ability to implement more advanced cyber security solutions, or to scale in line with emerging threats.

The COVID-19 pandemic prompted the firm to rapidly enable remote working for all staff, integrate multi-factor authentication (MFA), and enhance its overall security posture. The firm's preparedness for remote work also mitigated the impact of the war in Ukraine on its cybersecurity strategies. Both events were catalysts for progressing with new tooling and processes, reinforcing the firm's commitment to maintaining robust cybersecurity measures and adapting to emerging threats.

The firm is highly satisfied with its current cybersecurity model, especially given the outcome of incidents like the CrowdStrike cyber incident. They continuously monitor all systems, ensuring compliance with regulations such as GDPR and preparing for the upcoming NIS2 Directive. The cybersecurity measures have decreased the firm's risk profile, with cybersecurity being a permanent agenda item for the risk committee.

User compliance and awareness remain significant challenges. The firm emphasises user education and has implemented compulsory training programs to enhance cybersecurity awareness among employees. The culture surrounding cybersecurity within the firm is proactive, with constant evaluation and monitoring integrated into IT and operational processes.

The decision-making process for cybersecurity investments is primarily influenced by the Head of IT, with final decisions made by management team based on budget considerations and past outcomes. The firm is open to new ideas and continuously evaluates market trends and practices from similar firms to stay adaptable to changing threats.

Looking ahead, the firm plans to explore AI tools and other enhancements to improve its security posture. They maintain a proactive stance, ensuring that their cybersecurity strategies evolve with emerging trends and threats. The "no blame" culture and constant education approach have helped maintain high security awareness among staff, reinforcing the firm's commitment to robust cybersecurity practices.

In conclusion, this case study illustrates the measures taken by a mid-sized law firm in Ireland to adapt to the challenges posed by the COVID-19 pandemic and the war in Ukraine. The firm's hybrid cybersecurity model and, proactive user training, and comprehensive security culture have enhanced its resilience against evolving cyber threats, ensuring compliance and operational effectiveness in a dynamic environment.

## **7.3 Survey Results**

The survey results were grouped into logical sets in order to analyse further. The Configuration Manual contains further details. Each section was evaluated against firm size and specialisation.

### **7.3.1 Impact of COVID-19 and War in Ukraine on Cybersecurity**

Phishing attacks have become a significant concern for law firms since the onset of the COVID-19 pandemic. A notable 47% of respondents reported experiencing monthly phishing attacks, while 37% noted several phishing attacks per month. Annual phishing attacks were the least frequent, reported by 16% of firms. This indicates that phishing has become a persistent threat, likely exacerbated by the increase in remote work and digital communication during the pandemic.

Most firms (84%) reported never encountering Distributed Denial of Service (DDoS) attacks in the last four years. A smaller portion, 11%, experienced DDoS attacks at least once, and

only 5% reported frequent (annual) DDoS attacks. This suggests that while DDoS attacks are a known threat, they are relatively rare among the surveyed firms.

The perceived risk of state-sponsored cyberattacks varies among firms. A low extent of risk was perceived by 68% of respondents, 26% noted a moderate extent, and 5% perceived a high extent of risk. This indicates that while state-sponsored attacks are a concern, most firms do not see them as an imminent threat.

The transition to remote work during the COVID-19 pandemic has had varying impacts on cybersecurity. A low impact was reported by 53% of firms, while 32% experienced a moderate impact. Only 16% reported a high impact, and 5% noted no impact. This indicates that while the shift to remote work posed challenges, many firms adapted without significant disruptions to their cybersecurity posture.

Most firms (63%) reported never using personal devices for work during the pandemic. 21% reported rare usage, while 5% respectively noted occasional and very frequent usage. This suggests that the use of personal devices for work was not widespread, likely due to concerns about security and data protection.

The threat posed by inadequate home network security during remote work was considered low by 74% of firms. No threats were reported by 16%, while moderate and high extents of threats were noted by 5% each. This indicates that most firms had adequate controls for this threat.

Most firms (84%) managed increased cyber threats effectively during the pandemic, while 16% reported neutral management effectiveness. This suggests that firms were generally well-prepared to handle the heightened cyber threat landscape during COVID-19.

The comprehensiveness of cybersecurity guidance provided during the pandemic was moderately thorough by 79% of firms. Slightly comprehensive guidance was reported by 16%, while only 5% noted highly comprehensive guidance. This indicates that while most firms provided adequate guidance, there is room for improvement in making it more comprehensive.

The data suggests that while the COVID-19 pandemic and the Ukraine war have increased various cyber threats, law firms have addressed these risks meaningfully, demonstrating resilience and adaptability.

### 7.3.2 Current Cybersecurity Practices and Management

The data reveals that most firms (84%) consider their cybersecurity protocols adequate, with 16% perceiving them as neutral. All of the firms' report using multi-factor authentication (MFA) and regularly update their cybersecurity policies. Figure 6 illustrates the usage of MFA by size of firm.

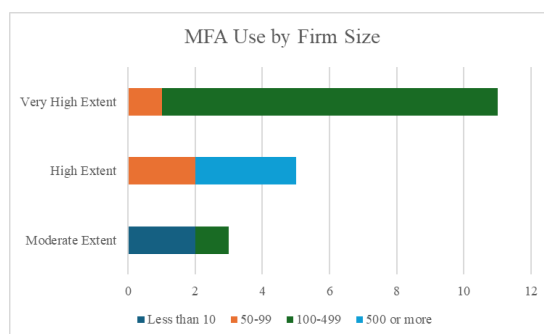
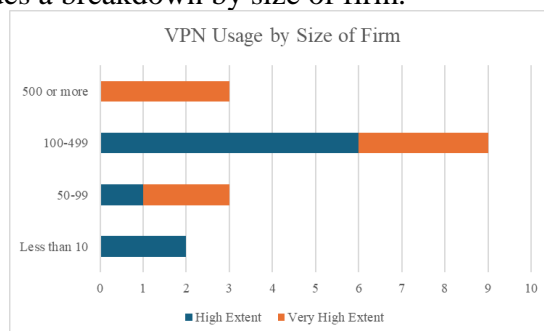


Figure 6. MFA Usage by Size of Firm

Cyber incident response plans are deemed effective by 84% of respondents. Employee training in cybersecurity is high, with all firms implementing this key control; over 30%

responded "High" or Very High" extents of training. Cybersecurity policy review is frequent in 63% of the firms, while 11% conduct reviews occasionally.

Collaboration with other firms for cybersecurity improvement is reported by 68% of the firms. Secure communication tools and VPNs are used by all firms who responded to this question. Figure 7 provides a breakdown by size of firm.



**Figure 7. VPN Usage by Size of Firm**

Confidence in handling future cyber threats is moderate, with 95% feeling moderately confident and 5% very confident.

The data indicates that law firms have established robust cybersecurity practices, with high adoption of MFA and frequent updates to policies. Employee training and collaboration are prioritised.

### 7.3.3 Use of Technology and Advanced Solutions in Cybersecurity

Law firms have increasingly integrated advanced technologies into their cybersecurity practices to mitigate risks and enhance protection. A significant portion of firms (63%) reported using AI in cybersecurity to a more than moderate extent, with 95% noting that AI effectively detects cyber threats. This reflects a commitment to leveraging advanced technologies to stay ahead of cyber threats. Over 90% of firms use real-time monitoring solutions.

In terms of defence against AI-enhanced cyberattacks, 21% of firms feel adequately prepared, highlighting a growing awareness of sophisticated cyber threats. However, encounters with AI deepfake scams remain relatively low, with 74% reporting rare or occasional attacks using this technique.

Observability tools for threat monitoring are widely used, with 95% of firms utilising these tools to at least a moderate extent. This is complemented by the use of SIEM platforms (58%) and either in-house or outsourced Security Operations Centres (SOCs) in 53% of firms. This combination ensures a comprehensive approach to real-time threat detection and response.

The frequency of reviewing observability data varies, with 58% of firms conducting reviews frequently, ensuring continuous monitoring and timely responses to potential threats. Metrics and logs are considered to be more than moderately comprehensive by 84% of firms.

Real-time monitoring solutions are deployed to a high extent by 90% of firms, enhancing their ability to detect and respond to threats swiftly.

The accuracy of threat insights from observability tools is considered moderately to highly confident by 95% of firms, reflecting the reliability and trust in these technologies.

The ability to detect anomalous behaviour is rated high by 37% of firms, while 37% also believe their observability tools are very effective in proactively identifying vulnerabilities.

Incident response times are significantly reduced in 32% of firms due to effective observability tools, highlighting the importance of timely action in cybersecurity.

Most firms in this dataset are medium to large-sized, with 74% having over 100 employees. The majority specialise in Corporate Law and other legal areas, indicating a diverse range of expertise within the legal industry. Many firms are based in both the UK and Ireland, with some having international operations. Most have been in operation for over 20 years, suggesting established practices and a strong foundation in the industry.

In conclusion, the data reflects a robust adoption of advanced technologies and a proactive stance towards cybersecurity among law firms.

### **7.3.4 Compliance and Risk Management**

Law firms have demonstrated a high level of GDPR compliance (90%) and preparation for the NIS2 Directive (79%). A high number of firms frequently conduct security audits (74%). All firms consider the legal implications of cyberattacks to be highly significant, underscoring the serious consequences of cybersecurity breaches in the legal sector. All firms reported their security measures to be effective, at a minimum.

The data also indicates that larger firms, especially those with over 500 employees and specialising in corporate law, are more likely to have very effective cybersecurity measures and comprehensive regulatory compliance. For instance, firms with over 500 employees, particularly those in corporate law, show a high frequency of security audits and an effective approach to EU regulation compliance. Additionally, firms specialising in corporate law, regardless of size, consistently report high effectiveness in their current cybersecurity measures.

In contrast, smaller firms, particularly those with less than 10 employees or specialising in family law, report less frequent security audits and a more neutral stance on the effectiveness of their cybersecurity measures. These firms often need more extensive resources and might benefit from targeted support to enhance their cybersecurity posture.

Overall, the data suggests that while there is a high level of awareness and proactive measures in place regarding cybersecurity among law firms, there is a noticeable variation based on firm size and specialisation. Large corporate law firms appear to be leading in comprehensive cybersecurity practices, while smaller firms may need additional resources and support to achieve similar levels of cybersecurity resilience.

### **7.3.5 Economic Impact and Investments**

The data reveals that law firms have generally reported a low extent of impact from cyber threats on their operational efficiency, with only 11% reporting a moderate impact and the remainder reporting low or none. Investment in cybersecurity for economic protection is frequent among these firms, with 63% making regular investments. The cost of recovering from cyberattacks is considered significant by a substantial portion of firms, with 58% marking it as at least highly significant. Most firms (89%) find their investment in cybersecurity effective or very effective in mitigating threats.

Large firms, especially those with over 500 employees and a focus on corporate law, consistently report a high frequency of cybersecurity investments and significant recovery costs. These established firms, often operating for over 20 years, demonstrate a strong commitment to maintaining robust cybersecurity measures. Their frequent investments are reflected in their high effectiveness in countering cyber threats, showcasing a proactive approach to securing their operations and client data.

In contrast, smaller firms, such as those with less than 10 employees, often report a very ineffective response to cyber threats and lower significance of recovery costs. These firms,

typically with lower revenues and fewer resources, might struggle more with the financial and operational impacts of cyberattacks. For instance, firms with less than 10 employees and specialising in real estate law often indicate lower impact and occasional investments in cybersecurity.

### **7.3.6 Decision-Making and Future Plans**

All firms (100%) reported having continuous monitoring for cyber threats in place. This unanimous adoption indicates the critical role that real-time threat monitoring plays in maintaining robust cybersecurity.

Frequent cybersecurity training is conducted by 79% of firms. This high frequency underscores the importance of ongoing education and training to maintain a high level of cybersecurity awareness among employees.

Most firms (89%) effectively incorporate incident feedback. This practice ensures that lessons learned from past incidents are used to improve future cybersecurity measures. Larger firms, particularly those with over 100 employees, report higher preparedness and more frequent investments in cybersecurity technologies. With greater resources, these firms can implement more comprehensive and regular cybersecurity measures compared to smaller firms, ensuring a more robust defence against potential threats. These firms, often specialising in corporate law and operating for over 20 years, show a robust cybersecurity posture. For instance, firms with 500 or more employees, particularly in corporate law, demonstrate very high investment and effective incorporation of incident feedback. Overall, the data suggests that while law firms are making significant strides in maintaining robust cybersecurity practices, there is variability based on firm size and specialisation.

### **7.3.7 Perceptions and Culture of Cybersecurity**

The data reveals that a substantial 79% of senior management teams understand the importance of cybersecurity investment, while 21% do not. Additionally, 63% of senior management teams actively support cybersecurity measures, indicating a strong organisational commitment to cybersecurity. This support is reflected in the fact that 95% of firms have cybersecurity on their senior management's agenda, emphasising the strategic importance placed on cybersecurity across the board.

Continuing the trend seen previously, larger firms, particularly those with over 100 employees, show a higher rate of understanding and support for cybersecurity investment. These firms, often specialising in various fields, including corporate law, and operating for more than 20 years, demonstrate a robust cybersecurity posture. For instance, firms with 500 or more employees, particularly in corporate law and international operations, show a very high extent of senior management support and understanding of cybersecurity investment. Overall, the data suggests that while law firms are making significant strides in maintaining robust cybersecurity practices, there is variability based on firm size and specialisation. Larger firms with more resources tend to have more comprehensive and frequent cybersecurity measures in place compared to smaller firms.

## 7.4 Discussion

The literature review highlights increased cyber risks faced by law firms due to recent global crises like COVID-19 and the war in Ukraine. Despite extensive research on cybersecurity, there is a gap concerning small to medium-sized law firms. This study addresses these gaps by examining cybersecurity challenges and strategies within law firms in Ireland and the UK, focusing on enhancing resilience through targeted research.

### Methodology

This study uses a quantitative survey method distributed via online platforms targeting diverse firms. Data was stored securely and anonymised further if required. Key steps included developing a questionnaire, distributing it, collecting responses, and analysing the data.

The survey employs a structured questionnaire with a 1-5 Likert scale and pilot testing. Data collection is online, encrypted, and anonymised. The Cybersecurity Threat Prioritisation Model (CTPM) categorises and ranks threats based on survey responses, providing actionable recommendations.

### Case Study 1

A mid-sized Irish law firm merged with a global firm, increasing cybersecurity investment and compliance. The hybrid model combines in-house and outsourced resources. COVID-19 and the war in Ukraine prompted enhancements in remote work security and cyber threat awareness. The firm uses a multi-tiered security approach, including SIEM systems, emphasising user training and a "security first" culture. Despite challenges like user compliance and false positives, the firm remains committed to continuous improvement and exploring AI tools.

### Case Study 2

Another mid-sized Irish law firm utilises in-house resources, an IT partner, and an external SOC for cybersecurity. The COVID-19 pandemic accelerated remote work capabilities and MFA integration. The firm, ISO27001 certified, employs a layered defence strategy. User education is a challenge, but compulsory training enhances awareness. The firm plans to explore AI tools and maintains a proactive stance towards emerging threats. The "no blame" culture supports high security awareness.

### Survey Results

Phishing attacks increased significantly, with many firms reporting monthly incidents. DDoS attacks were rare. Most firms perceived a low risk of state-sponsored attacks. Remote work had varying impacts, with many firms reporting minimal disruption. Personal device use for work was not widespread, and home network security threats were generally low. Firms managed increased cyber threats effectively.

Most firms consider their cybersecurity protocols adequate, with universal use of MFA. Cyber incident response plans are effective, and employee training is robust, with frequent policy reviews. Collaboration with other firms and secure communication tools are common. Confidence in handling future threats is generally high.

AI is widely used in cybersecurity and is proving effective. Real-time monitoring solutions are prevalent. Many firms employ SIEM platforms and SOCs. Observability tools for threat monitoring enhance the ability to detect and respond swiftly to threats.

Law firms demonstrate high GDPR compliance and preparation for the NIS2 Directive. Security audits are frequent. Larger firms, especially those with many employees, have comprehensive measures, while smaller firms may need more resources to improve their cybersecurity posture.

Cyber threats had a minimal impact on operational efficiency for most firms. Regular investments in cybersecurity are common. Recovery costs from cyberattacks are significant for many firms. Larger firms report higher investments and effective measures, while smaller firms face greater financial impacts.

All firms have continuous monitoring for threats. Frequent cybersecurity training and effective incorporation of incident feedback are common. Larger firms show high preparedness and frequent investments.

A substantial portion of senior management teams understand and support cybersecurity investment. Larger firms, especially those with many employees, demonstrate a strong commitment to cybersecurity.

## Recommendations based on Findings

The following table (Table 1) outlines key recommendations for law firms to enhance their cybersecurity posture, based on survey data, case studies, and findings from the literature review. These strategies aim to address both common and unique cybersecurity challenges faced by law firms, ensuring robust protection and compliance.

Recommendations	Details
Implement Comprehensive Phishing Awareness Programs	Regularly conduct phishing simulation exercises and provide targeted training sessions to employees. Develop clear protocols for reporting suspicious emails to ensure timely action.
Enhance MFA Adoption	Ensure MFA is implemented across all systems and for remote access to enhance security against unauthorised access.
Regular Cybersecurity Policy Reviews	Establish a routine schedule for reviewing and updating cybersecurity policies, ideally quarterly. Ensure policies are comprehensive and address the latest cyber threats and compliance requirements.
Increase Investment in Advanced Cybersecurity Technologies	Invest in AI-driven cybersecurity solutions for improved threat detection and response. Adopt SIEM systems and establish or outsource SOCs to enhance real-time monitoring and incident response capabilities.



Strengthen Remote Work Security Measures	Implement and enforce security protocols for remote work, including secure VPNs, endpoint protection, and regular security assessments of home networks. Provide training and resources for employees to secure their home office environments effectively.
Focus on User Compliance and Training	Conduct regular, mandatory cybersecurity training sessions for all employees, emphasising the importance of compliance and the latest threat landscape. Implement a "no blame" culture to encourage reporting of security incidents without fear of retribution.
Enhance Collaboration and Information Sharing	Participate in industry-specific cybersecurity forums and collaborate with other law firms to share best practices and threat intelligence. Establish partnerships with cybersecurity experts and consultants to gain insights and improve defences.
Develop a Cybersecurity Maturity Model	Create a framework to assess the firm's cybersecurity maturity level, identify gaps, and prioritise improvements. Use this model to guide strategic cybersecurity investments and measure progress over time.
Ensure Compliance with GDPR and NIS2 Directive	Regularly conduct security audits to ensure compliance with GDPR and prepare for the upcoming NIS2 Directive. Implement data protection measures and incident response plans that meet regulatory requirements.
Invest in Incident Response and Recovery Plans	Develop and regularly update comprehensive incident response and disaster recovery plans. Conduct tabletop exercises to test these plans and ensure readiness for potential cyber incidents.
Explore Emerging Technologies and AI Tools	Investigate the use of AI tools for proactive threat detection, anomaly detection, and automated incident response. Stay updated on emerging cybersecurity technologies and trends to maintain a cutting-edge security posture.
Increase Focus on Secure Communication Tools	Adopt and enforce the use of secure communication platforms for both internal and client communications. Regularly review and update encryption and secure messaging protocols.
Allocate Budget for Cybersecurity Investments	Ensure a dedicated cybersecurity budget to support ongoing investments in technology, training, and compliance. Consider cybersecurity investments as a critical aspect of the firm's overall risk management strategy.
Tailored Support for Smaller Firms	Smaller firms should seek targeted support and resources to enhance their cybersecurity capabilities, such as joining cybersecurity consortiums or leveraging government initiatives. Utilise managed security service providers (MSSP) for affordable access to advanced security solutions and expertise.

Table 2: Best practice recommendations for law firms

## Conclusion

Law firms are making significant strides in cybersecurity, but variability exists based on firm size and specialisation. Larger firms tend to have more comprehensive measures, while smaller firms may need additional support.

## 8 Conclusion and Future Work

This study set out to investigate the distinct cybersecurity challenges and the effectiveness of current mitigation strategies within law firms in Ireland and the UK, particularly in the wake of the COVID-19 pandemic and the war in Ukraine. The objectives were to examine the current

cybersecurity conditions, explore emerging challenges, evaluate existing defences, and propose actionable improvements tailored to the legal sector.

The research employed a quantitative survey method distributed to diverse small to medium-sized law firms, with data securely stored, anonymised, and analysed. The study successfully provided a detailed understanding of the cybersecurity landscape in the legal sector, revealing several key findings:

1. **Impact of COVID-19 and War in Ukraine on Cybersecurity:** Phishing attacks became a significant concern, with many firms reporting monthly incidents. Despite the rarity of DDoS attacks, firms perceived a low risk of state-sponsored cyber threats. Remote work introduced varying impacts, but many firms adapted without significant disruptions.
2. **Current Cybersecurity Practices and Management:** Most firms consider their cybersecurity protocols adequate, with universal use of MFA and effective incident response plans. Employee training and frequent policy reviews are standard, as is strong collaboration and the use of secure communication tools.
3. **Use of Technology and Advanced Solutions:** AI and real-time monitoring solutions are widely used and have proven effective in enhancing cybersecurity. Many firms employ SIEM platforms and SOCs, utilising observability tools for threat monitoring.
4. **Compliance and Risk Management:** High GDPR compliance and preparation for the NIS2 Directive were observed. Larger firms have more comprehensive measures, while smaller firms need more resources.
5. **Economic Impact and Investments:** Cyber threats had minimal impact on operational efficiency, with frequent investments in cybersecurity. Recovery costs are significant, and larger firms report higher investments and effectiveness.
6. **Decision-Making and Future Plans:** Continuous monitoring and frequent training are common. Larger firms show high preparedness and frequent investments, effectively incorporating incident feedback.
7. **Perceptions and Culture of Cybersecurity:** Senior management teams largely understand and support cybersecurity investment, especially in larger firms with a strong commitment to cybersecurity.

The study's findings indicate a robust approach to cybersecurity among law firms, though variability based on firm size and specialisation persists. Larger firms tend to have more comprehensive measures, while smaller firms may require additional support.

## 9 Future Work

While this research has provided valuable insights into the cybersecurity landscape of law firms, there are several areas for future work that could enhance the understanding and effectiveness of cybersecurity strategies:

1. **In-depth Qualitative Studies:** Future research could involve in-depth qualitative studies, such as interviews and focus groups, to gain deeper insights into the specific challenges and needs of small to medium-sized law firms. This approach would

complement the quantitative data and provide a more nuanced understanding of cybersecurity issues.

2. **Longitudinal Studies:** Conducting longitudinal studies to track changes in cybersecurity practices and threats over time would help identify trends and the long-term effectiveness of implemented strategies. This would be particularly useful in understanding the evolving nature of cyber threats and the impact of emerging technologies.
3. **Tailored Cybersecurity Frameworks:** Developing and testing tailored cybersecurity frameworks specifically designed for the legal sector could address law firms' unique vulnerabilities and requirements. This could include creating sector-specific guidelines and best practices for the legal industry's specific operational and regulatory contexts.
4. **Cybersecurity Training Programs:** Future work could focus on designing and evaluating comprehensive cybersecurity training programs for law firm employees. Assessing the effectiveness of different training methods and materials would help improve user compliance and awareness, reducing the risk of human error.
5. **Exploration of AI and Advanced Technologies:** Further research into integrating AI and other advanced technologies in cybersecurity could provide insights into optimising these tools for law firms. This includes evaluating such technologies' cost-benefit ratio and scalability in small to medium-sized firms.
6. **Policy and Regulatory Impact Studies:** Investigating the impact of cybersecurity policies and regulations on law firms would provide valuable information for policymakers. Understanding how regulations like GDPR and the NIS2 Directive influence cybersecurity practices and investments could guide the development of more effective regulatory frameworks.
7. **Collaborative Cybersecurity Initiatives:** Exploring collaborative cybersecurity initiatives between law firms, government agencies, and cybersecurity experts could lead to more robust defence mechanisms. This includes sharing threat intelligence, resources, and best practices to create a unified defence against cyber threats.

In conclusion, this study has successfully answered the research question and achieved its objectives, providing a comprehensive understanding of the cybersecurity challenges and strategies within law firms in Ireland and the UK. Future work should focus on enhancing the depth and scope of this research, addressing specific needs, and developing tailored solutions to improve the cybersecurity resilience of small to medium-sized law firms.

## References

- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, 9, 121916–121929.  
<https://doi.org/10.1109/ACCESS.2021.3109091>
- Aleksiev, M. Y., Bart Szewczyk, Anna Oberschelp de Meneses, Aleksander. (2023, January 17). *New EU Cyber Law “NIS2” Enters Into Force*. Inside Privacy.  
<https://www.insideprivacy.com/cybersecurity-2/new-eu-cyber-law-nis2-enters-into-force/>
- Ali, A., Khan, M. A., Farid, K., Akbar, S. S., Ilyas, A., Ghazal, T. M., & Al Hamadi, H. (2023). The Effect of Artificial Intelligence on Cybersecurity. *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1–7.  
<https://doi.org/10.1109/ICBATS57792.2023.10111151>
- Alwashali, A. A. M. A., Rahman, N. A. A., & Ismail, N. (2021). A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack. *2021 14th International Conference on Developments in eSystems Engineering (DeSE)*, 92–96.  
<https://doi.org/10.1109/DeSE54285.2021.9719456>
- Bencsáth, B., Pék, G., Buttyán, L., & Félegyházi, M. (2012). The Cousins of Stuxnet: Duqu, Flame, and Gauss. *Future Internet*, 4(4), 971–1003. <https://doi.org/10.3390/fi4040971>
- Biddle, S. (2016, August 19). *The NSA Leak Is Real, Snowden Documents Confirm*. The Intercept. <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/>
- Brantly, A. F., & Brantly, N. D. (2024). The bitskrieg that was and wasn't: The military and intelligence implications of cyber operations during Russia's war on Ukraine.

*Intelligence and National Security*, 39(3), 475–495.

<https://doi.org/10.1080/02684527.2024.2321693>

Cameron, S. (2023, May 12). *Singapore Passes Bill to Establish Information-Sharing Platform for Banks*. ComplyAdvantage.

<https://complyadvantage.com/insights/singapore-passes-bill-to-establish-information-sharing-platform-for-banks/>

Campobasso, M., & Allodi, L. (2020). Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 1665–1680. <https://doi.org/10.1145/3372297.3417892>

Chomiak-Orsa, I., Rot, A., & Blaike, B. (2019). Artificial Intelligence in Cybersecurity: The Use of AI Along the Cyber Kill Chain. In N. T. Nguyen, R. Chbeir, E. Exposito, P. Anrioté, & B. Trawiński (Eds.), *Computational Collective Intelligence* (Vol. 11684, pp. 406–416). Springer International Publishing. [https://doi.org/10.1007/978-3-030-28374-2\\_35](https://doi.org/10.1007/978-3-030-28374-2_35)

*Dashboard—EuRepoC: European Repository of Cyber Incidents*. (n.d.). Retrieved August 5, 2024, from <https://eurepoc.eu/dashboard/>

Davidson, R. (2021). The fight against malware as a service. *Network Security*, 2021(8), 7–11. [https://doi.org/10.1016/S1353-4858\(21\)00088-X](https://doi.org/10.1016/S1353-4858(21)00088-X)

Duneva, E. (2023). The impact of the war in Ukraine on cybersecurity. *InterConf*, 33(155), 35–40. <https://doi.org/10.51582/interconf.19-20.05.2023.003>

Gabrian, C.-A. (2022). HOW THE RUSSIA-UKRAINE WAR MAY CHANGE THE CYBERCRIME ECOSYSTEM. *BULLETIN OF “CAROL I” NATIONAL DEFENCE UNIVERSITY*, 11(4), Article 4. <https://doi.org/10.53477/2284-9378-22-92>

- Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, 36(1), 2037254. <https://doi.org/10.1080/08839514.2022.2037254>
- Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, 128, 103158. <https://doi.org/10.1016/j.cose.2023.103158>
- Hook, A., & Tangaza, H. (n.d.). *The use and regulation of technology in the legal sector beyond England and Wales*.
- Huaman, N., Acar, Y., Dreißigacker, A., & Fahl, S. (2021). *A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises*.
- Hussin, M. H., & Salwa Prilia Ginano, M. H. (2023). EUROPEAN UNION CYBER SECURITY IN DEALING WITH THE THREAT OF AI-CYBERCRIMES: LESSONS FOR INDONESIA. *Jurnal Dinamika Global*, 8(2), 192–212. <https://doi.org/10.36859/jdg.v8i2.1912>
- Jafar, M. T., Al-Fawa'reh, M., Barhoush, M., & Alshira'H, M. H. (2022). Enhanced Analysis Approach to Detect Phishing Attacks During COVID-19 Crisis. *Cybernetics and Information Technologies*, 22(1), 60–76. <https://doi.org/10.2478/cait-2022-0004>
- Jakobsson, A. K., & Nielsen, L. (2023). The cyber domain in the Ukraine War: A developed battlespace with proxy actors, escalation ladders and enemy labels. *Politica*, 55(1). <https://doi.org/10.7146/politica.v55i1.135835>
- Karo-Karo, G. F. M., Harumnanda, M. S. A., & Lim, C. (2023). Investigating Multiple Malware as a Service (MaaS): Analysis and Prevention Techniques. *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, 270–274. <https://doi.org/10.1109/ICoCICs58778.2023.10277515>

- Kim, D., Kwon, B. J., & Dumitraş, T. (2017). Certified Malware: Measuring Breaches of Trust in the Windows Code-Signing PKI. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 1435–1448.  
<https://doi.org/10.1145/3133956.3133958>
- Maestre Vidal, J., Sotelo Monge, M. A., Martinez Monterrubio, S. M., Barona Lopez, L. I., & Valdivieso Caraguay, A. L. (2019). Profits at the Dawn of Cybercrime-as-a-Service. *2019 International Conference on Information Systems and Software Technologies (ICI2ST)*, 71–78. <https://doi.org/10.1109/ICI2ST.2019.00017>
- Malatji, M. (2023). Offensive Artificial Intelligence: Current State of the Art and Future Directions. *2023 International Conference on Digital Applications, Transformation & Economy (ICDATE)*, 1–6. <https://doi.org/10.1109/ICDATE58146.2023.10248780>
- Mathew, A. (2023). Cybercrime-as-a-Service & AI-Enabled Threats. *International Journal of Computer Science and Mobile Computing*, 12(1), 28–31.  
<https://doi.org/10.47760/ijcsmc.2022.v12i01.004>
- Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, 92, 101762.  
<https://doi.org/10.1016/j.cose.2020.101762>
- Moore, T. (2019). BEST PRACTICES FOR STRENGTHENING THE CYBERSECURITY OF LEGAL INFORMATION ACROSS LAW FIRMS AND JURISDICTIONS. *Journal of Internet Law*, 22(12), 3–6.
- Ncubukezi, T. (2020). A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. 1–6. <https://doi.org/10.23919/ICITST51030.2020.9351339>
- Patsakis, C., Arroyo, D., & Casino, F. (2024). *The Malware as a Service ecosystem*.  
<https://doi.org/10.48550/ARXIV.2405.04109>

- Saalman, Dr. L., Su, F., & Saveleva Dovgal, L. (2023). *Cyber Crossover and Its Escalatory Risks for Europe*. SIPRI. <https://www.sipri.org/publications/2023/sipri-insights-peace-and-security/cyber-crossover-and-its-escalatory-risks-europe>
- Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. *Journal of Management Information Systems*, 34(4), 1023–1053.  
<https://doi.org/10.1080/07421222.2017.1394049>
- Schneider, M. (n.d.). *The Shadow Brokers—The story so far*. Retrieved July 25, 2024, from <https://www.scip.ch/en/?labs.20170511>
- Sembera, V., Paquet-Clouston, M., Garcia, S., & Erquiaga, M. J. (2021). Cybercrime Specialization: An Exposé of a Malicious Android Obfuscation-as-a-Service. 2021 *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 213–226. <https://doi.org/10.1109/EuroSPW54576.2021.00029>
- Shaikhanova, A. K., & Kadyrov, D. S. (2023). A Deep Dive into Cobalt Strike Tool. *Bulletin of Shakarim University. Technical Sciences*, 1(4(12)), 46–52.  
[https://doi.org/10.53360/2788-7995-2023-4\(12\)-7](https://doi.org/10.53360/2788-7995-2023-4(12)-7)
- Shanthi, R. R., Sasi, N. K., & Gouthaman, P. (2023). A New Era of Cybersecurity: The Influence of Artificial Intelligence. 2023 *International Conference on Networking and Communications (ICNWC)*, 1–4.  
<https://doi.org/10.1109/ICNWC57852.2023.10127453>
- Singh, J., & Rahman, N. A. (2023). Cybercrime-As-A-Service (Malware). 2023 *International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)*, 1–5. <https://doi.org/10.1109/EASCT59475.2023.10392459>



- Sitek, B. (2022). The Influence of Covid-19 on the Activities of Law Firms. *Teka Komisji Prawniczej PAN Oddział w Lublinie*, 15(2), 293–302.  
<https://doi.org/10.32084/tkp.4482>
- Somogyi, T., & Nagy, R. (2023). The Impact of the War in Ukraine on the Information Security of the European Union’s Banking Industry – A Case Study of Hungary And Slovakia. *CONTEMPORARY MILITARY CHALLENGES*, 25(3–4), 23–32.  
<https://doi.org/10.2478/cmc-2023-0020>
- Štručl, D. (2022). Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare. *CONTEMPORARY MILITARY CHALLENGES*, 24(2), 103–123. <https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6>
- Talukder, S., & Talukder, Z. (2020). A Survey on Malware Detection and Analysis Tools. *International Journal of Network Security & Its Applications*, 12(2), 37–57.  
<https://doi.org/10.5121/ijnsa.2020.12203>
- Tam, T., Rao, A., & Hall, J. (2020, December 23). *The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath*.  
<https://dl.acm.org/doi/fullHtml/10.1145/3436807>
- Teichmann, F., & Boticiu, S. (2023). The Importance of Cybersecurity Incident Response Plans for Law Firms. *Jusletter*, 1149.  
[https://jusletter.weblaw.ch/juslissues/2023/1149/the-importance-of-cy\\_3c77b063f1.html\\_\\_ONCE&login=false](https://jusletter.weblaw.ch/juslissues/2023/1149/the-importance-of-cy_3c77b063f1.html__ONCE&login=false)
- Teichmann, F., Boticiu, S., & Sergi, B. S. (2022). Ransomware – A Growing Threat for Law Firms. *Jusletter*, 1126. <https://doi.org/10.38023/d438edb2-e502-4a01-838a-896c7e43cb5a>

- The Bucharest University of Economic Studies, Bucharest, Romania., Paraschiv, D., Toader, L., Nițu, M., & Negrea, Ștefan. (2021). *Internet Fraud and Phishing Attacks—A European Perspective*. 394–400. <https://doi.org/10.24818/BASIQ/2021/07/051>
- The “Shadow Brokers” NSA theft puts the Snowden leaks to shame*. (2016, August 19). ExtremeTech. <https://www.extremetech.com/defense/234031-your-guide-to-the-shadow-brokers-nsa-theft-which-puts-the-snowden-leaks-to-shame>
- Van De Weijer, S., Leukfeldt, R., & Moneva, A. (2024). Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. *Computers & Security*, 139, 103693. <https://doi.org/10.1016/j.cose.2023.103693>
- Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information*, 6(2), 183–211. <https://doi.org/10.3390/info6020183>
- What is Mimikatz?* (n.d.). SentinelOne. Retrieved July 9, 2024, from <https://www.sentinelone.com/cybersecurity-101/mimikatz/>
- Zhuravka, A., Ageyev, D., & Chuhai, A. (2022). Some Questions of Cybersecurity in Ukrainian Modern Conditions. *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 579–582. <https://doi.org/10.1109/PICST57299.2022.10238611>