

# How OSINT can be used to improve the cyber posture of the construction industry

MSc Research Project

Rachel Hanlon

Student ID: X21189447

School of Computing  
National College of Ireland

Supervisor: Imran Khan


National College of Ireland  
MSc Project Submission Sheet

School of Computing

Student Name: Rachel Hanlon  
 Student ID: X21189447  
 Programme: MSc in Cyber Security Year: 1.5  
 Module: MSc Research Project  
 Supervisor: Imran Khann  
 Submission Due Date: 14<sup>th</sup> August 2023  
 Project Title: How OSINT can be used to improve the cyber posture of the construction industry  
 Word Count: 4907 Page Count: 19

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: 13<sup>th</sup> August 2023

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST**

Attach a completed copy of this sheet to each project (including multiple copies)	<input checked="" type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission,</b> to each project (including multiple copies).	<input checked="" 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 checked="" 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):	

## **Table of Contents**

<i>1</i>	<i>Introduction</i> .....	<i>2</i>
<i>2</i>	<i>Related Work</i> .....	<i>3</i>
2.1	The use of Open-Source Threat Intelligence (OSINT).....	3
2.2	Cyber incidents in the construction industry .....	3
2.3	Construction 4.0.....	4
<i>3</i>	<i>Research Methodology</i> .....	<i>5</i>
<i>4</i>	<i>Design Specification</i> .....	<i>6</i>
<i>5</i>	<i>Implementation</i> .....	<i>8</i>
<i>6</i>	<i>Evaluation</i> .....	<i>10</i>
6.1	Breakdown on results in the construction industry.....	10
6.2	Email security in the construction industry .....	10
6.3	Cyber posture across all organisations .....	11
6.4	Discussion.....	11
<i>7</i>	<i>Conclusion and Future Work</i> .....	<i>12</i>
	<i>References</i> .....	<i>13</i>
	<i>Appendix</i> .....	<i>15</i>

# How OSINT can be used improve the cyber posture of the construction industry

Rachel Hanlon

X21189447

## **Abstract**

*Vulnerability management is a tool that have been historically used in cyber management programs across all industries. OSINT is coming a new effect way to identify gaps in the cyber posture of an organisation and proactive harden the external defensive. OSINT is all publicly available information, meaning whatever the organisation can see, so can cyber criminals. Recently there have been many reports of construction companies suffering cyber breaches and there is a lot of talk nowadays about the evolution of construction 4.0. This research paper investigates if OSINT can be used to help improve the cyber posture of the construction industry.*

## **1 Introduction**

As we know vulnerability management is crucial part of any cyber program that a CISO or security manager would implement in order to improve the cyber posture of an organisation. Although vulnerability management can highlight both present and potential vulnerabilities on the network by using scanning tools such as Nessus, Qualys etc, the area of OSINT (Open-Source Threat Intelligence) is commonly overlooked. OSINT refers to information about cybersecurity threats and risks that is openly available and accessible to the public, it is often referred to as the "hackers eye view" of an organisation. However, it is also a method that can be used by competitors, customers, third party suppliers to verify the cyber posture of an organisation. This information is typically collected, analysed, and shared by various individuals, organisations, cybersecurity research and communities and published without any restrictions, allowing anyone to access, use and even contribute to the information. Construction 4.0 refers to the dramatic increased in use of technology within the construction industry. In recent years there has also been a significant increase in the number of cyber breaches within this sector, particularly business email compromise. It is believed that the construction industry remains a top target for cyber criminals due to the valuable data used, their high financial transitions, supply chain & 3<sup>rd</sup> party vulnerabilities, lack of cyber awareness, legacy systems, and remote work challenges. All these factors combine to create an environment where construction organisation is increasingly vulnerable to cybercrime. As the industry continues to digitise and adopt new technologies, it is crucial for the firms to understand the importance of cybersecurity and take proactive measures to safeguard their assets, employees, and operations.

This research paper combines the above two topics and investigates how to use of OISNT can aid a construction company to improve their cyber posture. Throughout this paper it becomes particularly evident that email security is the sectors largest downfall when it comes to their

cyber posture, OSINT highlights the simple and effective measures that can be taken to harden the email security barriers and better protect the industry.

Throughout this paper a deeper insight is taken into OSINT scanning and how it can be used effectively throughout day-to-day operations, the growing phenomenon of construction 4.0 and finally how the construction industry compares to other industries regarding the strength of their cyber posture.

## **2 Related Work**

### **2.1 The use of Open-Source Threat Intelligence (OSINT)**

Open-Source Threat Intelligence (OSINT) is widely used to gather details on an organisations cyber posture. Seokcheol Lee [1] used OSINT to inspect critical infrastructures by establishing an OSINT plan, preparing the data, collecting the open-source information, and generating security intelligence. By using this framework Lee was then able to improve the security level of the critical infrastructure as cyber threats that were not initially considered were then identified. In an alternative paper published by IJCSDF [4], OSINT was used to develop remediation techniques to help protect against cybercrime threats on social media. This review took gave an interesting insight into another area in which OSINT can be used to identify and remediate potential threats. By using similar techniques as Lee's paper [1] it was identified that although social media platforms are consistently being used for both social and business intelligence gathering, further research is required to gain deeper awareness to have the ability to mitigate threats and implement appropriate countermeasures. Although both papers showed that the use of OSINT had beneficial outcomes, they also show some limitations in the techniques that were used. This was evident due to the lack (or inability) or gather secondary data. Yadav, A, Kumar [6] proved this by using a combination of tools to provide accurate results. Using OSINT to gather information can result it wide range of data to be analysis, Rui Azevedo [2] developed a platform to collect OSINT feeds and normalise the data which was then separated into different modules. As a result of using this platform, Azevedo was able to identify 1174 IOC's (indicators of compromises) from data collected by just 34 organisations. The main benefit of using OSINT is to prevent a cyber-attack before it occurs, a study by Tundis [5] showed that standard alerts through automated features could be issued 32hours earlier meaning the average time to prevent a cyber threat can be increased when using OSINT. Although OSINT is mainly used to help identify potential vulnerabilities and prevent them before a cyber-attack occurs, it can also be misused by cyber criminals to identify weakness in potential targets which is a key finding in Isabelle Bohm's paper [3] when discussing the legal and ethical considerations of open-source intelligences.

### **2.2 Cyber incidents in the construction industry**

Although the construction industry is not usually known for their use of technology, this will be discussed later under 'construction 4.0', they continue to be a prime target for cyber-attacks. This is potential because the magnitude of money construction projects can cost, in some cases in trillions of euro range according to 'ToolSense' who recorded statistics and trends in 2023 [13]. The industry is known for dealing with high paying invoices and are a consist target of business email compromise. According to 'construction executive' [7] most of the recent ransomware attacks in the construction industry were caused by human error leading it to be ever so necessary to implement as many protection layers as possible such as

strong email security. Since 2019 internet security threat reports indicate that the construction industry was in the top 3 industries with a higher percentage of users targeted by malicious emails [8]. An article that was published in July 2022 surveyed a number of construction companies to see how many have experienced fraud in the past year [10]. A third of the organisations have fallen victim to invoice fraud and one in five firms have been subject to false billing, phishing attacks, and false expense reimbursements. Other notable cyber incidents in the construction industry include the Belfast based company ‘Lagan’ LockBit ransomware attack, the attack was announced on the dark web. The attack originated from a phishing email that tricked the recipient into downloading malware on the network [11], this attacked occurred in February 2023. Another notable cyber incident was the Barnes & Noble [12] breach which occurred in 2020, again another ransomware attack that occurred via a malicious email.

## 2.3 Construction 4.0

Construction 4.0 is a big change happening in how we build things and how the construction industry operates. This is becoming a widely used term across the world to talk about the new ways to use technology in construction operations. It’s about connecting the physical things we build with the digital world on the internet, the below diagram shows the important components that make up construction 4.0:

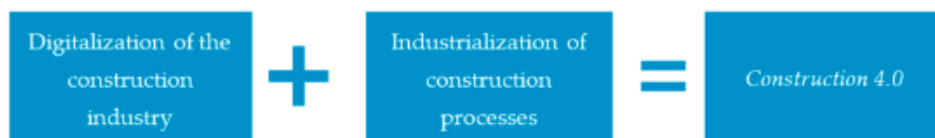


Figure 1 – Composition of Construction 4.0 [18]

It is important to highlight this term as part of the research project because, although the new wave of technology in the industry improves productivity, it also emphasizes the need to ensure they are secure. Construction stakeholders should be aware that moving more into the technology world brings more than a trendy new way of operations, it also brings a new range of risks that were not previously on the organisations radar. To conclude this review and draw a final understanding, 5 research papers were examined. These papers include a news article from “Building Transformations” [15], a research paper from the “University of Exeter” [14], an article from “Landform Surveys” [16], a paper from “Planning Building Construction Today” [17] and a research article titled “Construction 4.0: A Literature Review” written by “Eric Forcael” [18]. Together these papers helped to understand what people inside and outside the construction world think. From an analysis of the 5 papers the most popular technologies were identified:

- Internet of Things (IOT)
- Building Information Modelling (BIM)
- Virtual Reality
- Artificial Intelligence (AI)
- Drones

All the above technologies typically come with their own software which if not continuously kept up to date, can bring major risks to an organisation. Construction 4.0 may improve day to day operations but is also bring cyber security risks.

### 3 Research Methodology

OSINT can be completed manually through an individual investigation, but as discussed in the related work section of this paper there are available tools that can be used to make the process more efficient. An analysis was conducted on the top OSINT scanning tools of 2022 and 2023, the below list of tools was identified and chosen for further investigations:

- BlackKite
- BitSight
- SecurityScoreCard

To decide what tool would be best suited for the purpose of this research paper a comparison was compiled. This involved extensive research into each, and a free trial was used to scan an organisation on each tool so as the findings can be compared and the tool with the most effective findings could be identified. Included below is a high-level overview of the comparison:

Features	BlackKite	BitSight	SecurityScoreCard
Number of controls	290	40	105
Ease of scanning organisation	Very easy	Easy	Very Easy
Ease of use	Passed clear dashboard display	Passed	Passed
Knowledge base	Great	Good	Good
Licence cost	Mid expensive	Most expensive	Mid expense
Grading Methodology	Standards based	Proprietary and non-standard	Non-standard
RSI (Ransomware Susceptibility Index)	Yes	No	No
Dark Web Scanning	Yes	Yes	Yes
Digital footprint discovery (tool scans secondary domains that are found to be related to the primary)	Yes	No	No

Table 1 – OSINT tool comparison

From the above comparison it is evident that the BlackKite scanning tool was the ideal tool used for the purpose of this research paper. To kick off the investigation and begin the data analysis a BlackKite licence was purchased and billed on a monthly basis. This licence allowed for one organisation to be scanned at a time, therefore, once an organisation was scanned the results were inputted into a data analysis excel document that allow for all findings to be evaluated once the necessary scans were completed. It took the BlackKite tool approx. 24 hours to fully complete a scan on an organisation, as result is became a very lengthily process. If a CISO (Chief Information Security Officer) or security manager was to implement this process into their cyber program, BlackKite offer a portal that allows for the continuous scanning of multiple organisations which would be a far more efficient way to scan their own organisation as well as their 3<sup>rd</sup> parties.

BlackKite is an automated OSINT system scanning tool that provides real-time and accurate threat intelligence. The tool draws information using Shodan, Zoomeye, Censys and Dark

Web scanning, Web application scanning, public forms, and public searches to gain information on an organisation [19], this meant that the issue identified in section 2.1 of this paper of missing additional secondary data to back up OSINT findings could be overcome as the data was being collected from multiple sources. As previously mentioned, OSINT can be used by hackers to gain insight into the vulnerable areas of an organisation, it can be used to assess third parties & competitors, customers/clients can also use it to ensure their trusting a company with a high cyber posture. In this paper we will be using OSINT as a proactive approach to identify any common trends in the construction industry. To do this, several well known construction companies were scanned using BlackKite, although this is all publicly available information, the companies will be kept anonymous as the purpose of this research paper is not to hinder a organisations reputation but is to highlight how the use of OSINT can help an organisation improve their cyber posture and become better protected.

The OSINT scan provided a wide range of information, the chosen information modules to be included in the data analysis were:

- ❖ Cyber Rating
- ❖ Ransomware Susceptibility Index (RSI)
- ❖ Data Breach Index (DBI)
- ❖ Financial Impact Rating using FAIR (Factor Analysis of Information Risk)
- ❖ Number of corporate credentials leaked on the dark web
- ❖ Email Security protocols missing such as DMARC, SPF Records, DKIM
- ❖ SSL/TLS Strength Rating
- ❖ Attack Surface Rating
- ❖ Patch Management Rating
- ❖ Credential Management Rating
- ❖ DNS Health Rating
- ❖ IP Reputation Rating
- ❖ Email Security Rating
- ❖ Quantity of overall findings
- ❖ If the organisation has Windows 2008 Servers

The gathered data for the OSINT scan was then added into an excel document in order to begin analysing. Trends quickly began developing. To further the investigation a number of organisations from different industries were scanned so a comparison could be formed. These additional industries included Healthcare organisations, Law Firms, Government organisations, Technology, Manufacturing and entertain companies. This then allowed for the conclusion on whether the findings from the constructions companies were unique to the industry or if they were common weakness across multiple industries. To identify findings from the wide range of data that was in the data analysis excel, a number of graphs and tables were designed in order to highlight common trends.

## **4 Design Specification**

It is important to remember that OSINT scanning is all publicly available information and therefore only external and internet facing assets within an organisation are scanned. This is not a replacement for an internal vulnerability scan, it is however an addition to a vulnerability management program. OSINT can be described as similar to an external network penetration test, however the result shows the vulnerabilities whereas a penetration test would go an additional step and attempt to exploit the vulnerabilities. To decide on what companies were going to be used to draw data for this research paper, an investigation was conducted to identify the most well known organisation in each industry that was mentioned above as these organisations would likely be targets to cyber criminals. The construction



company was chosen to be the key area of focus for this paper as they have been the top target industry for cybercriminals over the past few years such to their lack of technical awareness. Historical construction companies were not involved in the digital world at all, whereas now with the emerging construction 4.0, technology is becoming a much bigger risk. Section 2 of this paper highlights that there have been many cyber breaches in the industry relating to malicious emails, this is a section of the OSINT scanning that was paid extra attention to in order to understand if the email security standard was lower than that of other industries.

BlackKite OSINT scanning tool breaks down the results into 19 module areas which can be seen below:

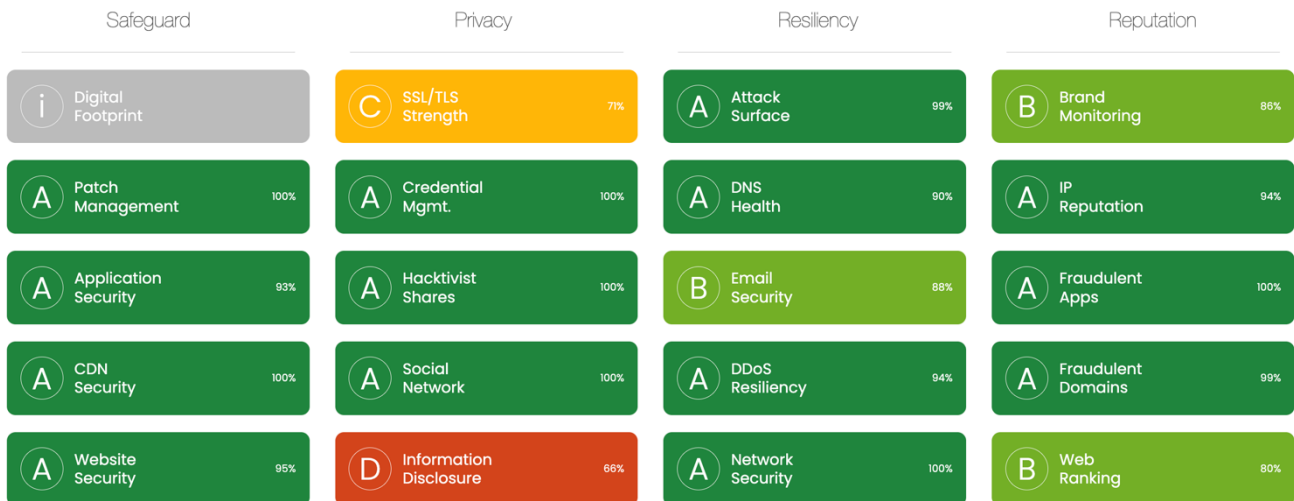


Figure 2 – Example of the Black Kite tool modules

BlackKite is a useful tool to understand what hackers can see of any organisation at any point in time. It uses OSINT, which stands for open-source threat intelligence, to gather useful information into an easy-to-read format, helping to priorities any findings. As previously mentioned, this information is freely available online and by collating we can gather the ‘hackers-eye-view’ of the organisation which helps security experts understand where to spend their valuable time in enhancing security controls. Many people believe hack attempts are always opportune events, however, this is not usually the case. If hackers see an opportunity to make money by extorting an organisation, they use automated tools to gather information in order to perform targeted attacks. The eco system attached to hacking is vast, operating like a well-tuned business. As a result, as opportunities are identified, this information can be sold onto cybercrime gangs with an SLA detailing how likely the hack is to succeed. Historically vulnerability management was prioritised to the internal network, however, it has become more commonplace for organisation’s to continually monitor their externally facing digital assets to react to any changes to the environment which may put them at risk there too as this is what is publicly visible.

BlackKite uses an A to F rating for each of the areas analysed but also to give an overall score. A security manager would always aim to be targeting an A+ score to give the organisation the highest possible chance to avoid an externally targeted security breach. In the case of these investigation many areas of the construction organisation’s fall below the rating of a “A+”. Research shows that those organisation’s which have a B rating are **3 times** more likely to be subject to a beach than those who have A ratings, C ratings are **5 times** more likely [19]. In technology environments, things change on a regular basis. Microsoft release patches once a month for example, as do many other technology providers.

Understanding if these vulnerabilities effect an organisation is paramount to ensuring and maintaining a highly security externally facing digital asset set in a similar way to how internal vulnerabilities are managed. It's imperative to understand if any of an organisation's users' credentials have been shared on the dark web also in order to assist with reacting to a security incident.

## 5 Implementation

In order to kick of the OSINT scan all that was needed was the organisations domain, which of course was simply to obtain for just running a Google search – showing just how easily this information can be obtained by just about anybody! How to initiate a scan is shown in detail in the manual that accompanies this report.

From the above section 4 we can see that the results are broken down into 19 different module areas, however there are also other pieces of information that were included in the data analysis are they provided good intel on the overall cyber posture of the organisation. Below is a breakdown of each area that was used in the data analysis and why:

### ❖ **Cyber Rating**

This is an overall score of the organisations cyber posture. It based on all the different areas described in section 2 of this manual.

### ❖ **Ransomware Susceptibility Index (RSI)**

This score shows how likely the organisation is to fall victim to a ransomware attack. Once scores improve across other modules areas of the organisation, the company will see the RSI score improve as a result of hardening the network defences.

### ❖ **Data Breach Index (DBI)**

This area provides insight into the frequency, impact and nature of data breaches across the company's industry and sectors, BlackKite then gives the organisation a DBI score based on how likely it is to suffer a data breach. For example, if there has been a recent data breach in the industry that was publicly disclosed and the organisation had a low information disclosure score (see above imagine of the module areas), a high DBI score can be expected.

### ❖ **Financial Impact Rating using FAIR (Factor Analysis of Information Risk)**

This is the likely cost of what a cyber breach would be if the organisation was to unfortunately suffer one.

### ❖ **Number of corporate credentials leaked on the dark web**

This was selected has it was felt that it highlights the end user awareness in the company, for example it appeared as many users were using their corporate email address for personal use websites judging by the source of where the credential was leaked onto the dark web from. Having corporate credentials leaked on the dark web also puts the organisation at a far gather risks as they will now be targeted by phishing emails and the cyber-criminal now knows the format of their email address – making it easier to spoof.

### ❖ **Email Security protocols missing such as DMARC, SPF Records, DKIM**

Each of these protocols will explain in detail in the evaluation section of this research paper. DMARC, SPF and DKIM are all important email authentication mechanisms used to enhance email security and combat email spoofing, phishing, and other forms of email-based

cyberattacks. Each protocol serves a distinct purpose in ensuring the authenticity of email communications and protecting both senders and recipients.

❖ **SSL/TLS Strength Rating**

Having a high score in this area is crucial for ensuring the security and privacy of data transmitted over internet. It is a protocol that provides encryption and authentication to ensure data is protected.

❖ **Attack Surface Rating**

This is the overall score of how well the organisation would be able to protect themselves from an attack.

❖ **Patch Management Rating**

Demonstrates how well the organisation systems are patched and kept up to date. Having out of date assets on the network makes the company vulnerable to many risks (depending on the asset).

❖ **Credential Management Rating**

This score is based on how many corporate credentials are leaked on the dark web.

❖ **DNS Health Rating**

Highlights the overall state, reliability, and security of a domains DNS (Domain Name System) infrastructure. If this score is show it can affect the company's reputation and leave them a target for cyber-attacks.

❖ **IP Reputation Rating**

Having a high rating in this area ensures the company can avoid blacklisting, keep a high business reputation, ensure email deliverability, keep a high level of website performance, etc.

❖ **Email Security Rating**

This score is pulled in from several factors such as credential management, missing email security protocols, is any assets relating to email functionality and missing patches.

❖ **Quantity of overall findings**

This measure was chosen to highlight the number of critical and high findings on the company.

❖ **If the organisation has Windows 2008 Servers**

Windows 2008 servers have now been unsupported for a long period of time. Having them on the network can leave the organisation exposed, hackers look for legacy servers on networks as a point of entry. The number of legacy assets on the external network also give an insight into what the internal network may look like.

To ensure a thorough analysis was performed, a total of 59 organisations across multiple industries was used.

## 6 Evaluation

As a result of running the OSINT scan on multiple organisations, not just in the construction industry, but across all sectors the results were very interesting and slightly surprising! As part of the data analysis the industries of construction, government, healthcare, and law were examined. In particular, an analysis was performed on the entire group of construction companies which shows the email to be quite low across all organisations. This aligns with section 2 of this research paper when it was shown that construction companies have suffered plenty of business email compromise in the past few years. A comparison was also completed on the cyber rating across all sectors.

### 6.1 Breakdown on results in the construction industry

The below graph visualises the average results across all construction companies that were scanned for this research paper. It is evident that the email security is the industry's weakest point due to the large number of credentials leaked on the dark web and the low scoring of the email secure strength. The patch management strength is also quite low which shows that the evolution of construction 4.0 has been implementing too many technologies and the industry cannot keep up with the patching and management. The overall cyber rating is in the high 80% which puts the industry in the 'B' rating, leading it to be 3 times more likely to suffer a breach than those with a 'A' rating.

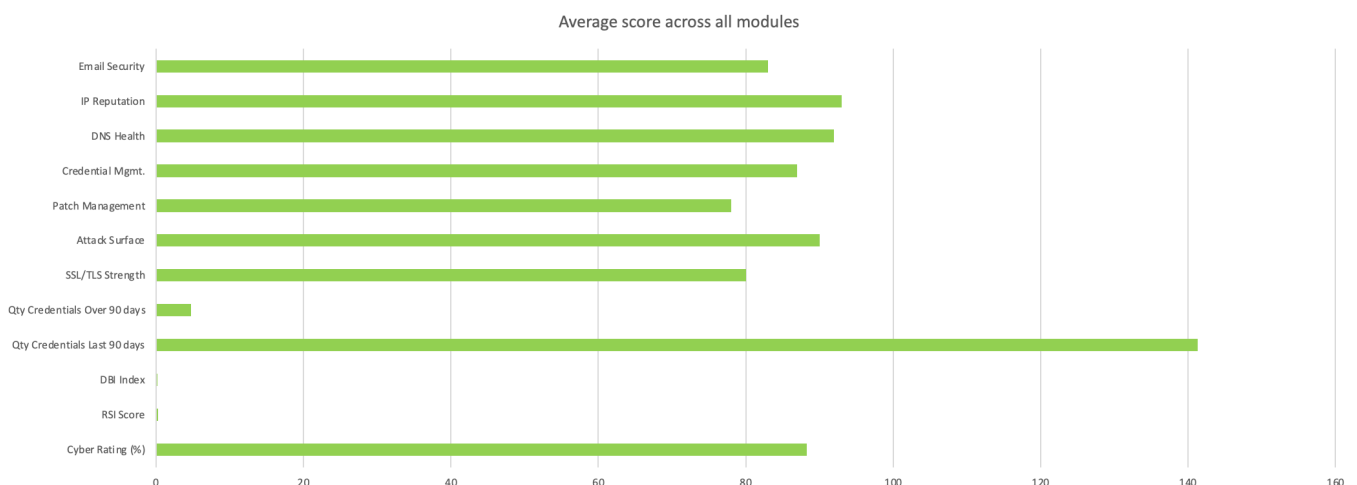


Figure 3 – Graph to demonstrate average score across all modules in the construction industry.

### 6.2 Email security in the construction industry

The results show that the average level of email security in the construction industry is lower than that of the healthcare, government, and law sectors (please see first graph in the appendix). The email security in the healthcare industry comes out as the highest, which is expected due to the volume of personal data they would be passing between departments and the public via email.

A deeper insight was taken into the email security area of the construction industry, it was discovered that many organisations are missing 1 and if not all 3 email security protocols, DMARC, SPF, DKIM (see pie in appendix). These 3 protocols are all very important authentication mechanisms that was used to protect the email from email-based cyber-attacks. Each protocol serves a different purpose:

- DKIM: DomainKeys Identified Mail (DKIM) was the protocol that was missing across most of the construction companies. If DKIM is not enabled, then our DMARC will also not work correctly. DKIM adds a digital signature to outgoing emails. This signature is generated using cryptographic keys associated with the sending domains. When the email is received, the recipient's server can verify that DKIM signature by checking the public key stored in the sender's DNS record and if the signature is valid, the email's identity is confirmed.
- SPF: Sender Policy Framework (SPF) is a DNS-based authentication protocol. It specifies which IP addresses or domains are authorised to send emails on behalf of the organisation domain. When an email is received, the recipient's mail server can check the SPF record to verify that the sender is legit and avoid falling victim to spoofing attacks and in turn blacklist your organisation's domain which will lead to email undeliverability and reputation damage.
- DMARC: Domain-based Message Authentication, Reporting and Conformance (DMARC) builds on the SPF record and DKIM by providing a policy framework for email authentication. It allows the organisation to specify what happens to incoming emails that fail the SPF and DKIM checks, i.e., quarantine, block the mails. DMARC also allows for the organisation to receive reports about email authentication failures which can in turn help to monitor and improve the email security. If your SPF and DKIM is not set up correctly, then the DMARC protocol will not operate as it should.

### **6.3 Cyber posture across all organisations**

Another key analysis that was conducted took a comparison of the average cyber ratings across all sectors. Surprisingly the construction industry done well in comparison to the law and government industries (see appendix). The Law industry was in the low 80s, Government hit the high 80s along with the construction industry and healthcare industry top the chart to the low 90s. It should be noted not none of these results are the ideal cyber rating!

### **6.4 Discussion**

The results from this research were interesting as they related to the previously work that was discussed in section 2 of this report. However, the results may have been slightly more accurate if organisations across Europe were used and not just Irish based companies, this would then allow to scan the same number of organisations across all the industries. For example, Ireland has a lot more law firms than construction organisations. Using the same number of organisations would allow for a more accurate average when comparing industry results. However, if that method was used, this for this research paper there would have had very little data to analyse.

Comparing the email security strength in the construction industry to the other sectors proved that this is a downfall in construction sector and not as a standard across all organisations. There are small steps that construction companies can take to improve the security in the area. Ensuring that the three email security protocols are enabled is a great step that is not too difficult or time consuming to implement and can provide a big deference in the security level. As the number of credentials leaked on the dark web is quite high, rolling out security awareness training to all users can also see a great benefit to the industry as users will become savvier as to handling their corporate emails address appropriately and spotting signs of phishing emails and business email compromise. These as quick and effective measure that can be taken by the industry.

More comparisons can be seen in the data analysis (Artefact) that accompanies this paper.

## **7 Conclusion and Future Work**

This research papers aim was to investigate how OSINT can be used to improve the cyber posture of the construction industry. Throughout the paper section 2 highlighted the most common form of cyber-attacks in the construction industry was email security-based attacks. When conducting the OSINT scans and analysing the results it was evident that the overall email security in the industry was lower than average. This proved that OSINT can be used to improve the cyber posture of the construction industry. This paper highlight how simply and effective OSINT is and should be introduced as an addition to all cyber programs.

The scope of this paper may have been slightly too broad, OSINT covers a very large range of areas and if the paper was to focus on one area i.e. email security, more time could have been spent on investigating different ways the email security could have been improved. Other options to improve/add on this research would be to conduct internal vulnerability assessments on the organisation and compare them to both the OSINT scans but then to also over all cyber scans and see if the results turn out the same, i.e., if an internal vulnerability scan was added to the data analysis, would the Law industry still come out with the lowest cyber rating?

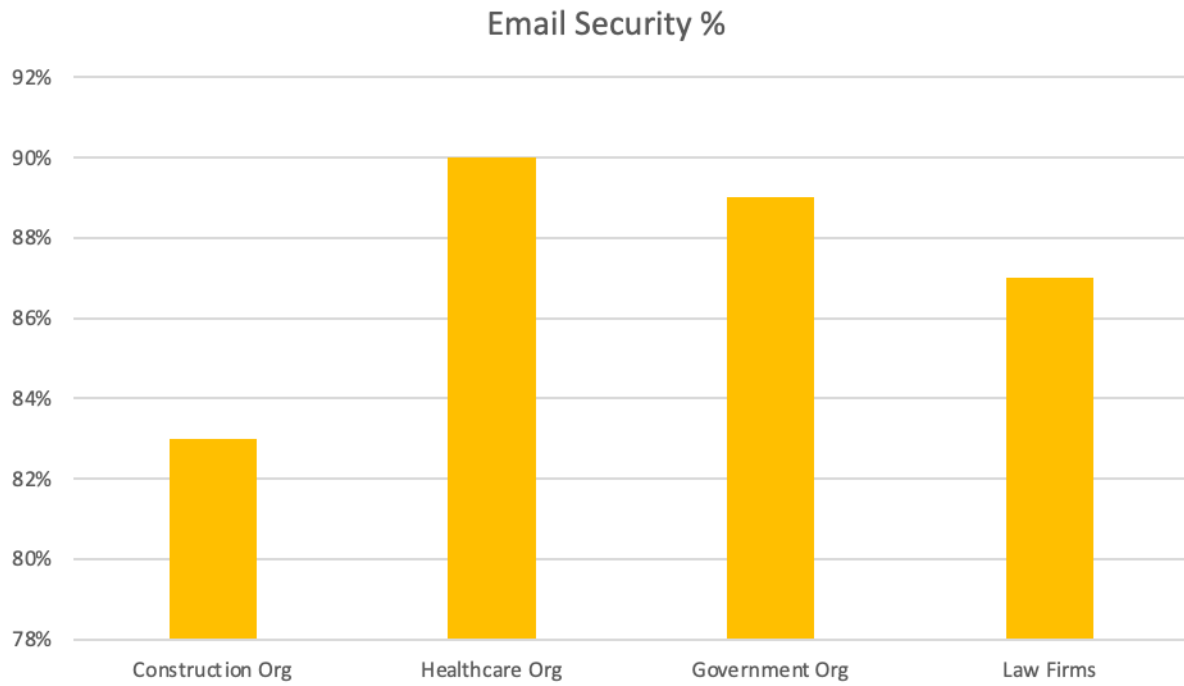
## References

- [1] S. Lee and T. Shon, "Open source intelligence base cyber threat inspection framework for critical infrastructures," *2016 Future Technologies Conference (FTC)*, San Francisco, CA, USA, 2016, pp. 1030-1033, doi: 10.1109/FTC.2016.7821730.
- [2] R. Azevedo, I. Medeiros and A. Bessani, "PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT," *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 483-490, doi: 10.1109/TrustCom/BigDataSE.2019.00071.
- [3] Böhm, I., Lolagar, S. Open source intelligence. *Int. Cybersecurity. Law Rev.* 2, 317–337 (2021). <https://doi.org/10.1365/s43439-021-00042-7>
- [4] Yeboah-Ofori, A. (2017) *Cyber Intelligence & OSINT: Developing mitigation techniques against ...* Available at: <https://repository.uel.ac.uk>
- [5] Tundis, A., Ruppert, S., Mühlhäuser, M. (2020). On the Automated Assessment of Open-Source Cyber Threat Intelligence Sources. In: Krzhizhanovskaya, V., *et al.* Computational Science – ICCS 2020. ICCS 2020. Lecture Notes in Computer Science(), vol 12138. Springer, Cham. [https://doi.org/10.1007/978-3-030-50417-5\\_34](https://doi.org/10.1007/978-3-030-50417-5_34)
- [6] Yadav, A., Kumar, A. & Singh, V. Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security. *Artif Intell Rev* (2023). <https://doi.org/10.1007/s10462-023-10454-y>
- [7] Hoeflinger, H. (2022) *The construction industry is more vulnerable than ever to cyber attacks, Construction Executive | Welcome*. Available at: <https://www.constructionexec.com/article/the-construction-industry-is-more-vulnerable-than-ever-to-cyber-attacks>
- [8] García de Soto, B. (2022) *Understanding the Significance of Cybersecurity in the Construction Industry: Survey Findings, ASCE Logo, redirects to the Home Page Search term(s) Search Journal*. Available at: <https://ascelibrary.org/doi/full/10.1061/%28ASCE%29CO.1943-7862.0002344>.
- [9] R. K. Manthaa, B. (2019) *Cyber security challenges and vulnerability assessment in the ...*, *Creative Construction Conference* . Available at: <https://repositorium.omikk.bme.hu/bitstream/handle/10890/13197/CCC2019-005.pdf?sequence=1>
- [10] Tansley, E. (2022) *1/4 UK construction companies experienced fraud in last year, TWinFM*. Available at: <https://www.twinfm.com/article/a-quarter-of-uk-construction-companies-have-experienced-fraud-over-the-last-year>
- [11] McAleer, R. (2023) 'Belfast construction firm targeted by group behind Royal Mail ransomware attack', *The Irish News*, 21 February.

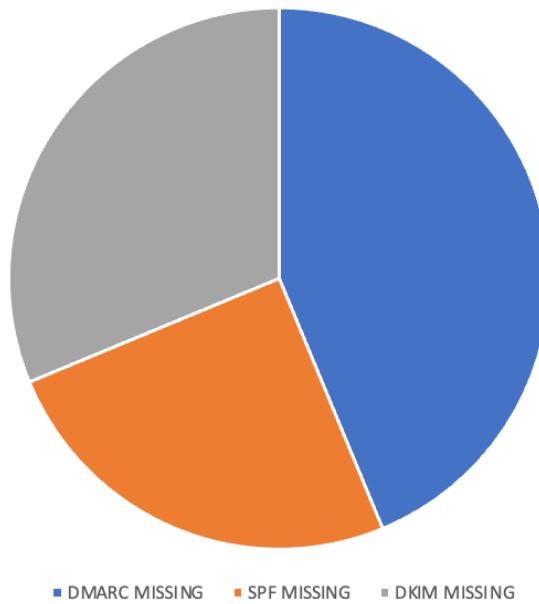
- [12] Osborne, C. (2020) *Barnes & Noble confirms cyberattack, Ransomware Group Leaks allegedly stolen data*, ZDNET. Available at: <https://www.zdnet.com/article/barnes-noble-confirms-cyberattack-customer-data-breach>.
- [13] ToolSense (2023) *Construction Industry Statistics and trends 2023*, ToolSense. Available at: <https://toolsense.io/studies-reports/construction-industry-statistics-and-trends/> (Accessed: 10 August 2023).
- [14] Construction 4.0 technologies key to improving sustainability of sector (2022) Articles | Research and Innovation | University of Exeter. Available at: [https://www.exeter.ac.uk/research/news/archive/2022/articles/title\\_895671\\_en.html](https://www.exeter.ac.uk/research/news/archive/2022/articles/title_895671_en.html)
- [15] Boton, C. (no date) *Construction 4.0 the next revolution in the construction industry, The next revolution in the construction industry*. Available at: <https://www.buildingtransformations.org/articles/construction-4-0>
- [16] Hinds, E. (2023) *Rising technology trends in construction*, Landform Surveys. Available at: <https://www.landform-surveys.co.uk/news/the-rising-technology-trends-in-construction/>
- [17] Hazlegreaves, S. (2022) *The evolution of technology within construction*, Planning, Building & Construction Today. Available at: <https://www.pbctoday.co.uk/news/digital-construction/construction-technology-news/technology-within-construction/105552/>
- [18] Forcael, E. *et al.* (2020) *Construction 4.0: A literature review*, MDPI. Available at: <https://www.mdpi.com/2071-1050/12/22/9755>
- [19] *Third Party Risk Management Software & Solutions* (2023) Black Kite. Available at: <https://blackkite.com/>



# Appendix



### Missing Email Security Protocols in Construction Organisations



### Cyber Rating Comparison

