January 2024

Cybercrime and cybersecurity practices in the Middle East construction industry

Freshfields | Accuracy | جامعة نيويورك ابوظبي NYU ABU DHABI | CENTER FOR CYBER SECURITY | LexisNexis | RICS

Contents

Introduction 4

Executive summary 8

Findings 10

Recommendation 16

Methodology 19

Conclusion 23

Contents

Introduction

Executive Summary

Findings

Recommendation

Methodology

Conclusion

Introduction

Cybercrime is a growing concern for the construction sector in the Middle east

Amidst the rise of cybercrimes and cyberattacks, it has become paramount for companies across the globe to prioritise the establishment of strong cybersecurity measures.

Freshfields Bruckhaus Deringer, Accuracy, and New York University Abu Dhabi (***NYUAD***) collaborated to carry out a comprehensive survey within the Middle East region's construction sector (the ***Survey***). The purpose of the Survey was to evaluate the risks construction project participants face in relation to cybercrimes and gauge their level of preparedness.

This report examines the common cybercrime and cybersecurity practices in the Middle East construction sector using the results from the Survey. In addition to this introductory section, the report is structured as follows:

- Section II sets out the executive summary.
- Section III sets out the key findings from the Survey, including highlighting risks that make the sector more vulnerable.
- Section IV sets out our recommendations on best cybersecurity practices, including mitigation strategies, for the construction sector based on the data and findings gathered from the Survey.
- Section V explains the methodology adopted to gather and analyse the Survey data.
- Section VI provides our conclusion and key takeaway points from the Survey findings.

The Construction Industry Is Vulnerable to Cyber Attacks

Around the world, the construction sector has been hit hard by the rise of cybercrime in recent years. To take one example, Dutch construction company Royal Bam Group fell victim to cyberattacks in 2020 when cyber criminals encrypted the company's data, preventing access to it. The company had to take a number of its systems offline in order to neutralise the attack.[1] Indeed, the increasing digitalisation of construction processes has given cybercriminals new opportunities to target construction project participants, who now hold increasingly large amounts of sensitive data in online repositories. Despite increasing reliance on digital processes, cybersecurity awareness within the sector remains relatively low. This vulnerability is evident from a 2021 survey,[2] which highlighted the sector's susceptibility to cyberattacks and the elevated success rates for such attacks.

At the same time, cybersecurity has not gained much attention from construction researchers, as demonstrated in an academic study.[3] The Survey's findings shed light on the scale and scope of the issue and highlight the urgent need for construction project participants to take cybersecurity seriously.

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

1 Construction News. (2020). "Bam Construct and Interserve hit by cyber attacks": https://www.constructionnews.co.uksections/contractors/bam-construct/bam-construct-hit-by-cyber-attack-13-05-2020/

2 García de Soto et al. (2022). Understanding the Significance of Cybersecurity in the Construction Industry: Survey Findings. Journal of Construction Engineering and Management, 148(9), 4022095. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002344

3 Sonkor, M. S., & García de Soto, B. (2021). Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. Journal of Construction Engineering and Management, 147(12), 4021172. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002193

Why Should Companies Care about Cyber Incidents Targeting the Construction Sector in the Middle East

While companies in all industries are susceptible to cyberattacks, the somewhat unique aspects of the construction sector's complexity of projects, layers of stakeholder involvement, emphasis on time efficiency, and heavy reliance on sensitive personal and business data can make the impact of cyberattacks on construction sector companies particularly harmful. Companies in the Middle East are at even greater risk, given the close relationship they may have with government entities on projects or the increasing rate of growth in the area, which is not always accompanied by a proportionate investment in cybersecurity. In particular, we note:

- **Construction projects** require time efficiency. Time is money on a construction project, with the risk of delays contractually allocated within the supply chain. Therefore, a cyberattack that imperils the diligent progress of a project can have significant ramifications.
- **Construction projects rely on sensitive data**. Plans and designs used for construction can provide information regarding access points and weaknesses in security for the finished structure. That is sensitive data, particularly during the operations phase of the project (for example, if special airport systems could be accessed during operations because of unknown hacks during the design and construction phase).
- **Construction projects have complex supply chains**. There can be very lengthy supply chains on construction projects, with even the lowest level of the supply chain having access to plans, designs, and other sensitive data. To protect the project's data, every layer of the supply chain needs to be focused on cyber security, but smaller entities at the bottom of the supply chain will not have the same ability to invest in cyber security.
- **Political sensitivity is greater in the Middle East**. Many construction projects in the Middle East are financed by government or private entities in which the state has invested (or owns). That can create a political dimension to (a) the need for cybersecurity (in addition to data protection laws, there may be a licensing regime pertaining to data relating to a project procured by government – e.g., DESC in Dubai) and (b) the motivation for cyberattacks.
- **There is increasing technological reliance in the Middle East**. Historically, technology adoption on construction projects in the Middle East has been slow, but it is now ramping up. In particular, a 2022 PwC Middle East Capital Projects and Infrastructure Survey identified that technology adoption in the construction sector has surpassed 50% for the first time.[4] If technology is not adopted in concert with suitable cybersecurity measures, the construction sector in the Middle East will continue to face problems.

Key Areas of Concern: Theft of Sensitive Data and Ransomware Attacks

One of the most common forms of cybercrime in the construction sector is the theft of sensitive data, which can be used for purposes of ransomware, identity theft, access to trade secrets, etc. Stolen data can include plans, designs, project management information, and personal and financial data. This data loss can have financial implications, put projects at risk, and harm the company's reputation.

Another primary concern is the threat of ransomware attacks. A study by Nordlocker showed that construction had been the most targeted sector by ransomware attacks in 2022.[5] In these attacks, cybercriminals encrypt a company's data and demand payment in exchange for the decryption key. The construction sector is particularly vulnerable to such threats due to the intricate data landscape tied to construction projects, which often holds significance for project success.

4 See "PwC Middle East 2022 Capital Projects & Infrastructure Survey" PwC (November 2022), available at https://www.pwc.com/m1/en/publications/capital-projects-and-infrastructure-survey-report/capital-projects-and-infrastructure-survey-report-2022.pdf (accessed on 4 September 2023).

5 Nordlocker. (2021). Top industries hit by ransomware. Nordlocker. Available at: https://nordlocker.com/recent-ransomware-attacks/

Quantifying Cyber Incidents Is Difficult Because Many Incidents Are Unreported

Accurately gauging the prevalence of cyberattacks within the sector poses a challenge, given that many incidents go unreported despite the existence of data protection legislation mandating data breach reports in certain circumstances. The frequency and severity of attacks can vary widely depending on the industry and global region.

However, there is no doubt that cyberattacks have become a significant problem for businesses across all sectors and one that is growing. In recent years, there have been high-profile attacks on companies in industries such as healthcare, finance, retail, technology, and construction. For instance, in 2019, a Canadian construction company fell victim to a severe ransomware attack, during which the attackers demanded a ransom of USD 6.5 million to release 60GB of crucial data.[6] Similarly, in 2020, a French construction company experienced a cyberattack that resulted in malicious actors gaining control of over 200GB of sensitive data and demanding a ransom of USD 11 million. As a precautionary measure, the company had to temporarily shut down multiple operational systems, leading to significant project delays.[7]

According to a report by Cybersecurity Ventures, the global cost of cybercrime is projected to reach USD 10.5 trillion by 2025. The report also estimates that a new cyberattack occurs every 11 seconds, with attacks increasing rapidly.[8]

Another report by the Ponemon Institute found that the average cost of a data breach in the United States was USD 9.05 million in 2021. The report also found that the average time to identify and contain a breach was 287 days.[9]

In summary, cyberattacks present a significant and growing threat to businesses in all sectors across the globe, including in the construction sector in the Middle East. The financial and reputational costs of such attacks can be substantial. Project participants must therefore invest in robust cybersecurity measures and stay vigilant against emerging threats.

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

6 CBC News. (2020). Ransomware attack on construction company raises questions about federal contracts. Available at: https://www.cbc.ca/news/politics/ransomware-bird-construction-military-1.5434308

7 Bouygues. (2020). Press Release – Information on a Cyberattack. Available at: https://www.bouygues.com/wp-content/uploads/2020/01/prbouyguesconstructioncyberattack01-31-2020-pdf.pdf

8 Cybersecurity Ventures. (2020). Cybersecurity Ventures' Cybercrime Report Predicts Cybercrime Damages Will Cost The World $10.5 Trillion Annually By 2025. Available at: https://www.cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

9 Ponemon Institute. (2021). 2021 Cost of a Data Breach Report. Available at: https://www.ibm.com/downloads/cas/OJDVQGRY

Executive summary

The Survey set out to identify the cybercrime prevention practices and cybersecurity risks in the Middle East construction sector. Conducted among respondents occupying senior roles primarily in large companies across the Middle East region, the Survey highlighted a concerning reality: even sizable companies lack the necessary readiness to effectively fend off significant cybercrimes. Incidents of phishing scams, ransomware attacks, and data breaches had already affected the surveyed companies. Recent media coverage has further emphasised the substantial losses that could stem from cyberattacks targeting the construction sector.

The Survey findings indicate that even large companies with resources at their disposal feel that they are not adequately prepared to address or prevent cyber incidents, and many indicated that they do not have sufficient measures in place to mitigate cyber risk. Tackling and averting these threats demands concerted action. Companies must shield their networks, devices, and data through concentrated efforts in employee training, policy implementation, and adequate investment in cybersecurity technology.

Indeed, to protect against cybercrime, construction project participants need to implement robust cybersecurity measures. This includes educating employees on cybersecurity best practices, using strong passwords and two-factor authentication, and regularly backing up data. Collaborating with cybersecurity experts is equally pivotal, enabling companies to identify vulnerabilities and enact appropriate security measures. These measures are particularly important for companies in the construction sector in the Middle East, given the complexity of construction projects and increased sensitivities of their data, supply chains, and stakeholders. Increased reliance on technology in the construction sector in the region makes the need for robust cybersecurity measures even more critical.

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

Findings

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

Demographics of Survey Respondents

Country Distribution

The Survey was conducted across multiple countries in the Middle East and some countries outside the region. In the Middle East, responses were received from companies in the United Arab Emirates, Saudi Arabia, Qatar, Jordan, Egypt, Oman, Bahrain, and Iraq. See Figure 1 for the distribution of the respondents' countries.

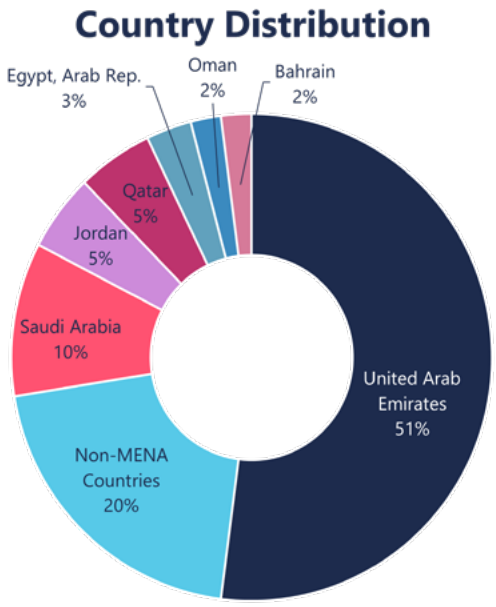


Figure 1. Distribution of the survey respondents' countries

Demographics of Survey Respondents

Company Size

The Survey respondents were from a broad spectrum of company sizes, ranging from micro businesses to large enterprises. Most respondents (70%) represented companies with over 250 employees (Large Companies). By contrast, approximately 17% represented companies with 50–249 employees (Medium Companies), 8% represented companies with fewer than ten employees (Micro Companies), and 5% represented companies with 10–49 employees (Small Companies) as shown in Figure 2.

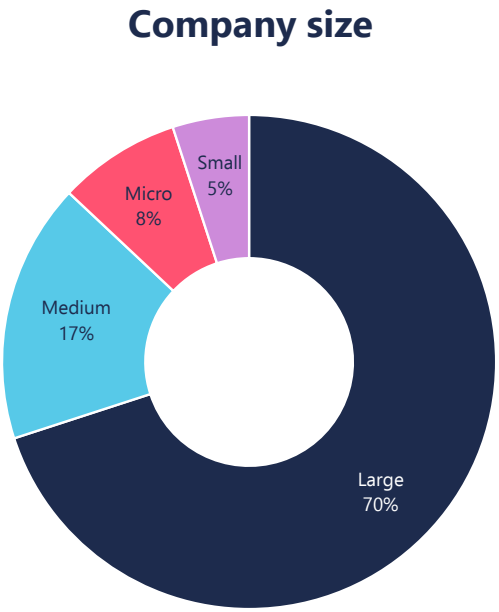


Figure 2. Distribution of the survey respondents' company sizes

Seniority

The Survey collected responses from individuals of varying seniority levels within their company: senior management represented 34%; manager or advisor level respondents, approximately 27%; and non-managerial senior employees, 25%. The remaining 14% of respondents were high-level senior management, entry-level employees, or others. Figure 3 shows the distribution of survey respondents' seniorities.

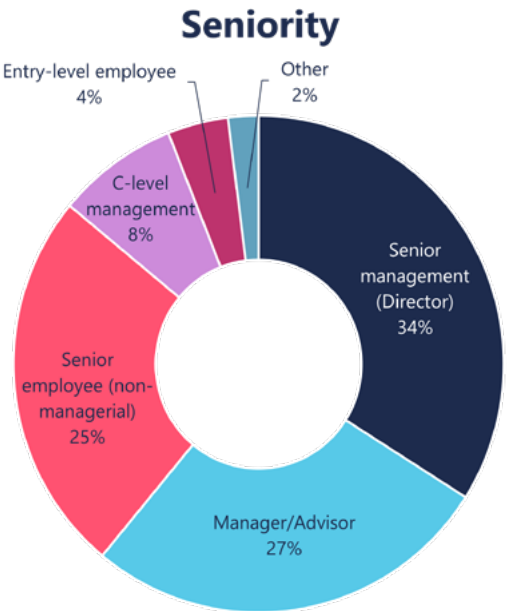


Figure 3. Distribution of the survey respondents' seniorities

Scope of Companies

The Survey collected responses from various project participants involved in the construction sector, including project managers, contractors, owners, suppliers, architects, and designers. Most respondents (20%) represented project management, while approximately 25% represented contractors and sub-contractors. The remaining respondents represented roles such as owners, partners, stakeholders, engineers, designers, and architects, as seen in Figure 4.

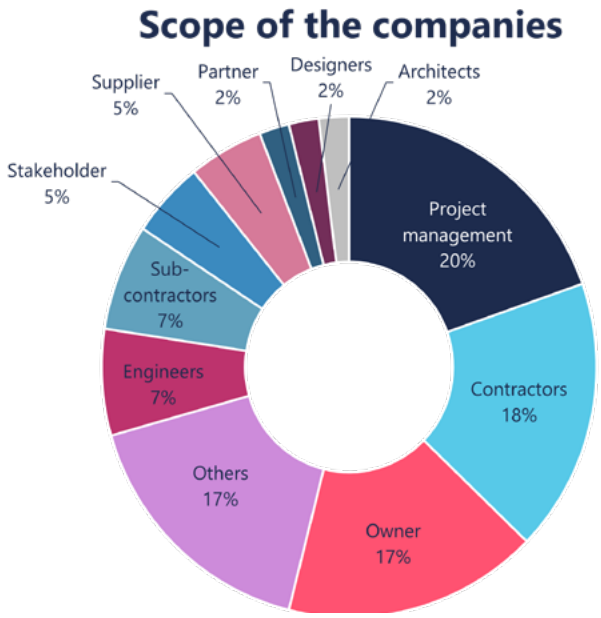


Figure 4. Distribution of the survey respondents' company scopes

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

The Construction sector is particularly vulnerable to cyberattacks

The construction sector has long been recognised as traditional, implementing technology more slowly than many others. In a 2016 report by McKinsey, it was listed as the second least digitalised industry after agriculture and hunting.[10]

However, the sector's gradual integration of technology, coupled with its insufficient cybersecurity safeguards, has rendered it an increasingly attractive target for cybercriminals. The Survey results highlight the alarming prevalence of cybercrime and cyberattacks within the sector and underline the need for project participants to prioritise cybersecurity.

Types of Cyberattacks in Construction

The Survey results indicate that the types of cyberattacks on the increase in the construction sector are phishing scams, ransomware attacks, and data breaches. The escalation of these attacks is largely attributed to the impact of COVID-19. These attacks can lead to the loss of sensitive information, financial losses, and disruptions to the construction process, resulting in delays and additional costs.

The Verizon 2020 Data Breach Investigations Report pinpoints social engineering schemes[11] as one of the leading cyber threats faced by the construction industry. It involves cyberattackers impersonating senior management and key vendors through business email compromise (BEC) tactics. Their goal is to convince victims to transfer funds or provide sensitive information that can be exploited for financial gain.[12]

Lack of Preparedness

The Survey results also reveal that the lack of preparedness is not limited to smaller project participants. Large project participants with substantial resources are often unprepared to tackle cyber threats, with many lacking the necessary cybersecurity measures and resources to protect themselves from potential cyberattacks. The previously mentioned 2021 academic survey[13] found that only 39% of construction sector companies had a cybersecurity plan, highlighting the need for the construction sector to place an increased emphasis on cybersecurity.

The Survey found that a significant proportion of respondents expressed concern about cybersecurity in the construction sector. Specifically, 34% of respondents were significantly concerned about cybersecurity, while 41% were somewhat concerned. These figures underline that the majority view cybersecurity as an imperative matter demanding attention or perceive their construction businesses as inadequately equipped to handle it.

A key obstacle to preparedness is awareness and knowing how to navigate risks. When asked about their employer's understanding of cybersecurity, 34% of respondents to the Survey reported being very well aware of cybersecurity, while 41% had some knowledge about it. This suggests that many construction business owners recognise the importance of cybersecurity but may benefit from additional support to develop their understanding further.

The Survey also revealed that only 24% of respondents reported a significant investment in cybersecurity, and only 27% stated their investment was sufficient. As many as 27% of respondents said that their investment in cybersecurity was insufficient, indicating a need for more resources dedicated to cybersecurity within the construction sector.

10 Agarwal, R., Chandrasekaran, S., & Sridhar, M. (2016). Imagining construction's digital future. McKinsey&Company, Exhibit 1.

11 Social engineering schemes are cyberattack tactics which involve manipulating, influencing, or deceiving a victim to gain control of a computer system or steal personal or financial information.

12 Verizon. (2020). 2020 Data Breach Investigations Report. Available at: https://www.verizon.com/business/resources/T753/reports/2020-data-breach-investigations-report.pdf

13 García de Soto et al. (2022). Understanding the Significance of Cybersecurity in the Construction Industry: Survey Findings. Journal of Construction Engineering and Management, 148(9), 4022095. https://doi.org/10.1061/(ASCE)CO.1943-7862.0002344

When asked if their employer periodically conducts cybersecurity risk assessments, the responses were more evenly spread: 37% of respondents said 'yes', indicating that their employer takes cybersecurity seriously and takes steps to assess potential risks; 31% of respondents said 'no', indicating that their employer does not conduct cybersecurity risk assessments; and 32% did not know or were not sure, highlighting a potential gap in cybersecurity knowledge within the construction sector.

With cybercrime on the rise, construction companies must prioritise cybersecurity education, resources, and policy implementation to protect their networks, devices, and sensitive data from cyber threats. By adopting a comprehensive set of security measures and working with cybersecurity experts, project participants can mitigate the risk of cyberattacks and protect themselves and their business partners from potential harm.

Investing in Cybersecurity

The impact of cybercrime on the construction sector has become a growing concern due to the shift towards digitalisation and remote work. The results of the Survey provide insights into the perceptions of construction sector professionals on the impact of various factors on cybercrime, including human intervention, cybersecurity regulations, national jurisdictions, investigative capabilities, and company financials. Additionally, in this section, we examine the extent to which project participants have policies and procedures in place for addressing cybercrime.

Human Intervention Plays a Key Role in Cybercrime

Human intervention plays a crucial role in both perpetuating and preventing cybercrime. As technology advances, the actions, behaviours, and attitudes of individuals towards technology significantly affect their vulnerability to cybercrime. Most cyberattacks, such as weak passwords, social engineering, or phishing scams, exploit human error or negligence.

According to a 2022 report prepared by Verizon, human factors played a significant role in 82% of approximately 2,250 global data breach incidents.[14] This emphasises the decisive influence of human engagement in cybercrime. The same report further highlights that attackers primarily breach security defences by employing malware and capitalising on stolen credentials. This pattern of human-centric cyberattacks is just as prevalent in the EMEA region – where stolen credentials accounted for over 65% of the avenues through which attackers gained unauthorised access – as it is globally.[15]

The majority of respondents to the Survey (76%) believe that human intervention has a critical impact on cybercrime. This further underlines the importance of employee training and education in preventing cyberattacks, ultimately reducing the risk of cyberattacks, as employees are often the first line of defence against cybercrime.

Cyber Regulations and Company Policies and Culture Work Together to Create Effective Cybersecurity Environments

Regulations in tandem with company prioritisation of cybersecurity are key to combatting cybercrimes. When asked about the impact of cybersecurity regulations on cybercrime, 37% of respondents said it has a significant effect, while 52% said it has a slight impact. When asked about the broader regulatory and socio-cultural context, 35% of respondents said the location where you do business can significantly influence cybercrime, while 46% said it has a slight effect.

These findings advocate for a comprehensive approach in which companies wield a pivotal role in cultivating a climate that champions effective cybersecurity regulations. This concerted effort is crucial in preventing and combatting cybercrimes, further emphasising the role of organisations in shaping a protective cybersecurity culture.

14 Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Page 33. Available at: 2022-data-breach-investigations-report-dbir.pdf (verizon.com)

15 Verizon. (2022). 2022 Data Breach Investigations Report (DBIR). Page 82. Available at: 2022-data-breach-investigations-report-dbir.pdf (verizon.com)

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

Committing Financial Resources and Taking Investigative Steps Are Key to Preventing and Detecting Cyberattacks

The Survey findings suggest that financial resources and investigative capabilities are essential in preventing and detecting cyberattacks. More than half of respondents (57%) believe that investigative capabilities have a significant impact on cybercrime, while 26% said it has a slight impact. Additionally, 52% of respondents said that a company's financial investment in cybersecurity significantly affects cybercrime, and 39% said it had a slight effect.

Policies and Procedures Related to Dealing with Cybercrime

In response to questions about policies and procedures concerning cybercrime, 48% of respondents confirmed having such measures in place. This indicates that the majority of surveyed project participants are actively equipped with policies to safeguard against cyber threats. However, 22% of respondents said 'no', suggesting a potential oversight of this facet of cybersecurity in certain companies. Meanwhile, 30% of respondents did not know or were unsure, highlighting the need for increased awareness and education about cybercrime prevention and response.

Cybercrime and COVID-19

The COVID-19 pandemic caused significant disruption across various sectors, including construction. The transformation towards remote work and amplified dependence on technology spurred the rise of cybercrime as a pressing concern.[16]

Impact of COVID-19 on Crime in the Construction Sector

In the Middle East, COVID-19 had a recognised impact on cybercrime incidence. When asked about the impact of the pandemic on crime in the construction sector, the responses were as follows:

- 29% of respondents reported a significant increase in crime.
- 31% of respondents reported a slight increase in crime.
- 23% of respondents reported that crime remained about the same.

Yet, only 13% of respondents reported that their businesses significantly changed existing cybercrime prevention measures because of COVID-19; 25% said no changes were made at all.

Impact of COVID-19 on Business Vulnerability to Cybercrime

The pandemic also had a significant impact on the vulnerability of construction businesses to cybercrime. When asked about the effect of COVID-19 on their business's exposure to cybercrime, the respondents answered as follows:

- 15% reported a significant increase in vulnerability.
- 67% reported a slight increase in vulnerability.

Types of Cybercrime Experienced or Observed

The Survey also asked respondents about the types of cybercrime they experienced or observed from the start of the pandemic. The results were as follows:

- 73% of respondents reported a significant or slight increase in phishing and social engineering attacks.
- 25% of respondents reported no change in malware and virus dissemination, 23% reported a significant increase, and 35% reported a slight increase.
- No respondents saw any decrease in denial-of-service attacks, business email compromises, social media hacks and spamming, electronic money fraud, sales fraud, identity theft, and credit card fraud.

The Survey findings indicate that the COVID-19 pandemic had a notable impact on cybercrime in the construction sector, with a significant number of respondents reporting an increase in cyberattacks. They also suggest that businesses became more vulnerable to cyberattacks during this period, with the prevalence of phishing and social engineering attacks standing out as the most commonly experienced or observed cybercrimes.

16 Interpol. (2020). COVID-19 cyberthreats. Available at: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

Recommendation

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

The first line of defence against any cyber threat, including in the Middle East construction sector, is increasing perception and awareness from the top: 'prevention is better than cure'. Most companies could improve value and security by adopting a proactive approach from upper management to tackle cybercrime-related risks.

Such an approach towards cybercrime risk management typically requires a cultural shift – this starts with board-level executives who can incorporate cybercrime-related risk into their enterprise risk strategy. In doing so, leaders can quickly identify gaps and steer the organisation towards a holistic approach in countering cyber threats.

Further, companies should focus on building a sustainable and multi-tiered approach to risk management rather than the piecemeal approach often taken today. A sustainable process starts with a risk assessment. A suggested framework for conducting such an assessment is outlined in Figure 5 and Figure 6.

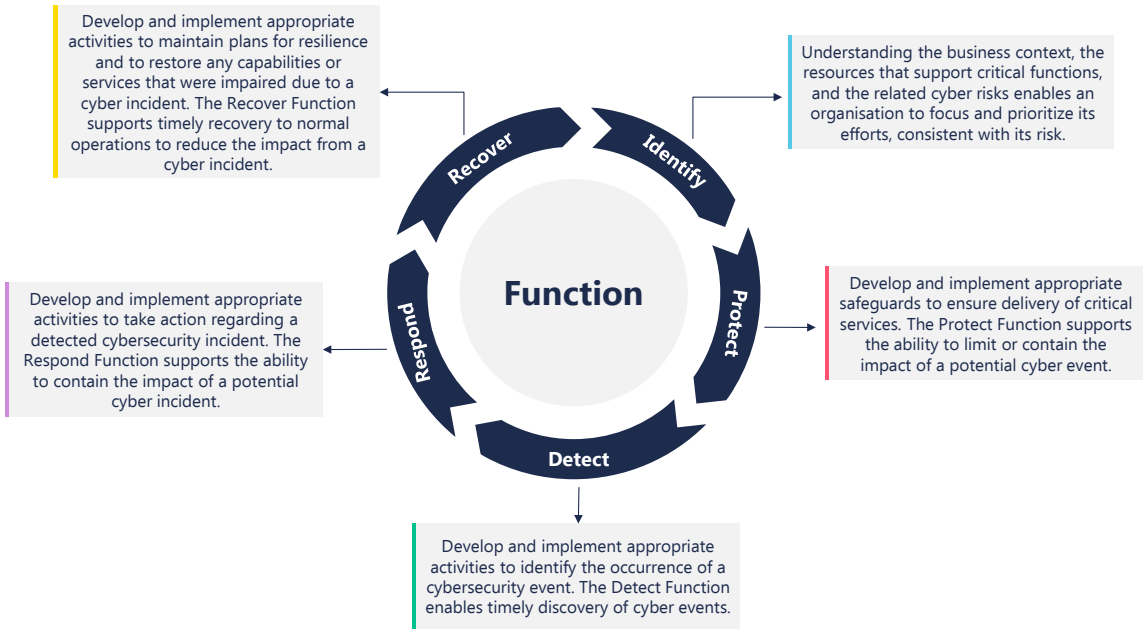


Figure 5. The suggested risk assessment framework (functions)

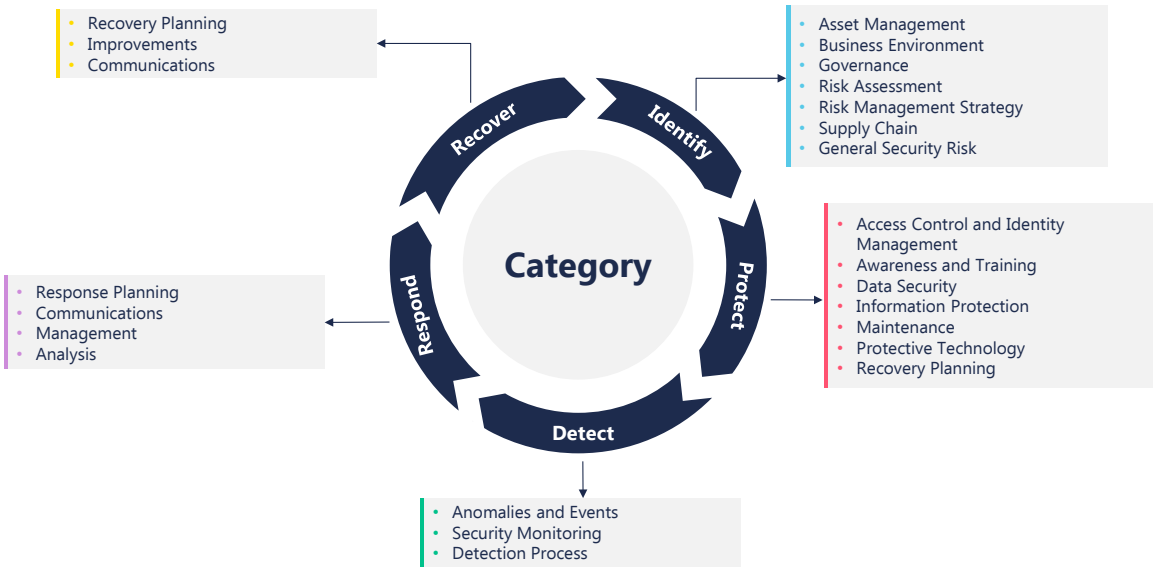


Figure 6. The suggested risk assessment framework (categories)

Several cybercrime deterrents are commonly utilised to prevent and alleviate the harm caused by cybercrime. Moreover, various post-breach measures can be implemented to manage and curtail the consequences of a cyberattack or data breach. These include, but are not limited to:

Technical Controls

These measures are designed to prevent unauthorised access to computer systems, networks, and data. Technical controls include firewalls, intrusion detection and prevention systems, anti-virus software, encryption, and access controls.

In the event of a cyberattack or data breach, companies must first seek to contain the breach and limit further damage by working with legal counsel and the IT team on a plan to isolate affected systems and devices and update security measures and protocols.

Policies, Procedures, Processes, and Best Practices

Policies and procedures are put in place to govern the use of computer systems and data. These may include acceptable use policies, password policies, data backup and recovery policies, and incident response plans.

Legal counsel can assist companies with developing plans to address vulnerabilities in processes and corporate policies, which may contribute to a breach, and assist with updating policies and procedures. Legal counsel may also recommend that a company subject to a breach conduct an internal investigation to identify the cause, extent, and impact of the breach.

Training and Awareness

Employees and users of computer systems need to be trained in recognising and avoiding cyber threats. Training can include security awareness training, phishing simulations, and regular reminders of best practices.

Legal and Regulatory Controls

Laws and regulations can provide a framework for cybercrime deterrence. These may include data protection laws, data breach notification requirements, cybercrime laws providing criminal penalties for cybercriminals, and licensing requirements for dealing with data on government-procured projects.

In the event of a cyberattack or data breach, a company may need to take measures to comply with regulatory requirements or respond to regulatory inquiries (among other actions). Once data breaches occur, legal counsel can be effective in advising on requirements to notify regulatory agencies and affected individuals in accordance with data protection laws.

Collaboration and Information Sharing

Collaboration between organisations, government agencies, and law enforcement can help to identify and respond to cyber threats more effectively. This can include sharing threat intelligence, best practices, and resources.

Overall, an effective cybercrime deterrent strategy should be comprehensive and include a combination of technical controls, policies and procedures, training and awareness, legal and regulatory controls, and collaboration and information sharing.

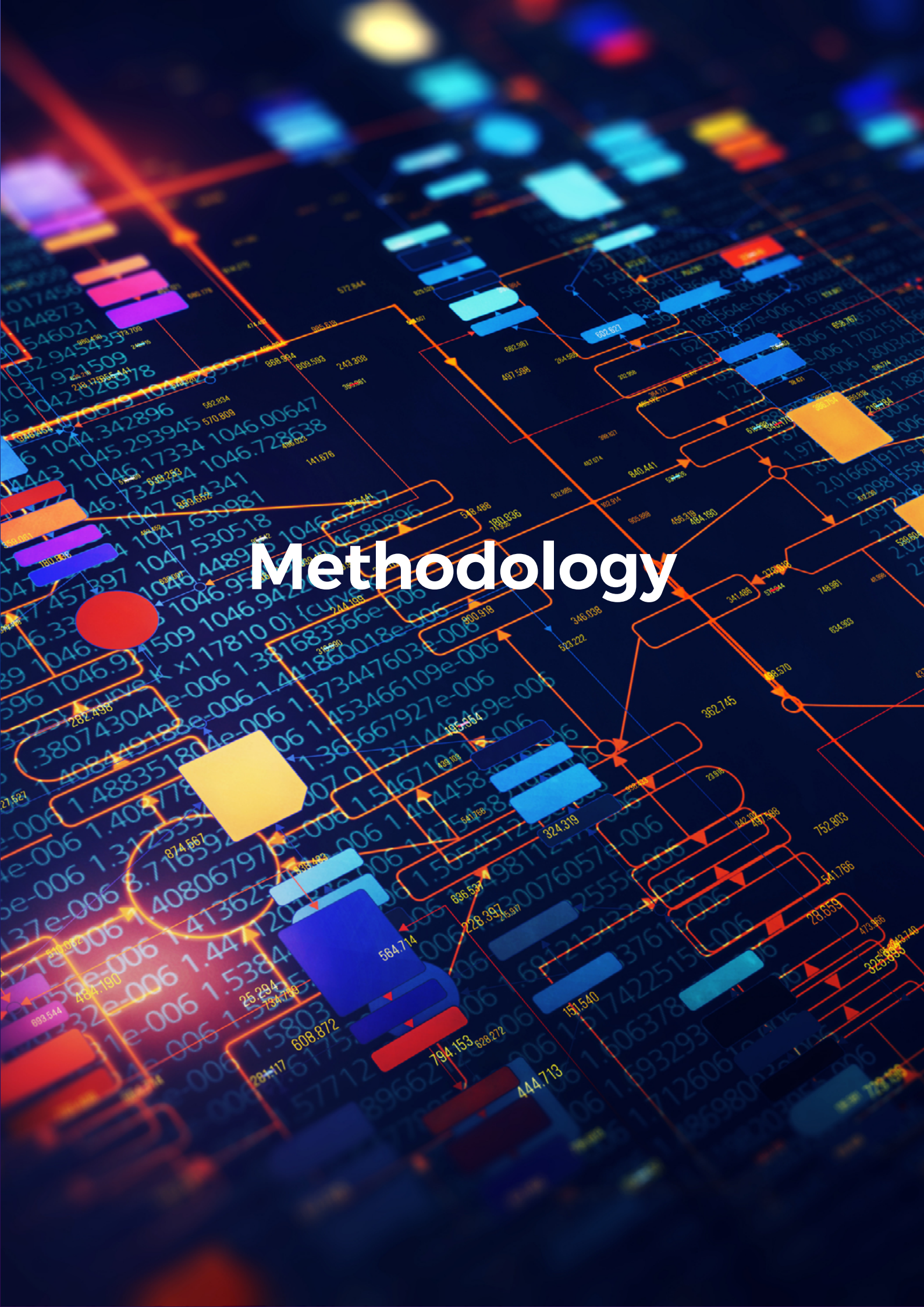
Investing in Cybersecurity Measures

To address the issue of cybercrime in the construction sector, project participants must prioritise cybersecurity. They must invest in the necessary measures to protect their assets and operational integrity. This comprehensive effort encompasses the adoption of a multi-faceted cybersecurity strategy that covers employee training, leverages technology, and enforces effective policies.

Collaborating with cybersecurity and cybercrime experts can help project participants stay attuned to the evolving cyber threats landscape. This proactive approach enables them to implement appropriate countermeasures to mitigate risks. A National Institute of Standards and Technology report recommends that project participants conduct regular risk assessments, implement security controls, and establish incident response plans to protect against cyber threats.[17]

Companies should always seek to invest in their cybersecurity capabilities to ensure they are sufficiently protected from cyberattacks. However, in the unfortunate event of a breach, having a well-conceived plan is imperative to navigate the intricate and often stressful aftermath with precision.

17 National Institute of Standards and Technology. (2019). NIST SP 1800-13A Cybersecurity Practice Guide: Securing the Industrial Internet of Things (IIoT): Cybersecurity for Distributed Energy Resources. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-13A.pdf



Methodology

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

The methodology for the Survey's design, deployment, and analysis is summarised in five steps, as shown in the flowchart in Figure 7. The details of each step are shown below.

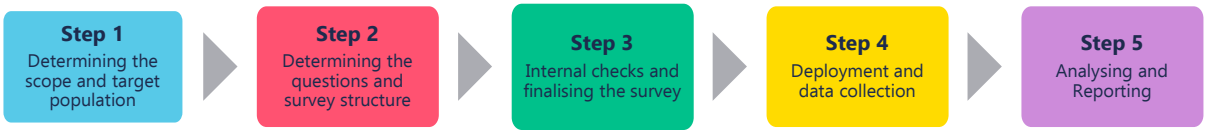


Figure 7. Flowchart for the Survey's methodology

Step 1 – Determining the scope and target population

The first step of designing a survey is to decide on the scope based on the research questions to be answered. These questions will also determine the target population since the focus will indicate who should participate in the survey.

In this Survey, the scope encompassed a range of objectives. This entailed the identification of cyber risks targeting the construction sector, understanding the level of awareness and preparedness of project participants, and assessing the impact of COVID-19 on the prevalence of cybercrimes. The Survey mainly targeted construction sector professionals predominantly in the Middle East region to keep the study focused and draw conclusions more accurately.

Step 2 – Determining the questions and survey structure

The second step is to write questions that effectively address the established research inquiries and align with the survey's defined scope. The questions should be relevant to the target population since some might be unnecessary in specific geographic areas or professional roles. The way of distributing the survey, such as via email, an online survey platform, or in person, should also be decided at this stage since it might affect the type of questions.

It was decided that the Survey would be conducted via an online survey platform, Qualtrics, to reach the maximum number of participants in the target population. It consisted of six sections: (1) Demographics, (2) Organisational and Industry Approach to Technology, (3) Cybersecurity Awareness, (4) Cybercrime Approach, Policies, and Procedures, (5) Cybercrime and COVID-19, and (6) Respondent's Information. The first and the last sections sought insights into each respondent's characteristics and that of their employer, such as the size and scope of work of the respondent's employer and the respondent's level of seniority. The second section included questions to identify the types of technology utilised by the respondents' companies. Sections three and four aimed to gauge the cybersecurity awareness of the respondents, their concerns related to cybercrime, and their employers' preparedness to combat potential cyber threats. Finally, the fifth section included questions to measure the impact of COVID-19 on the cybercrime landscape in the construction sector, particularly in the Middle East region.

Step 3 – Internal checks and finalising the survey

This step aims to perform checks to detect any potential flaws, assess the clarity of the questions and effectiveness of the survey structure, and optimise the survey length to achieve the maximum number of complete responses. Since three different organisations conducted the Survey, each organisation performed the checks and provided feedback from their perspectives and using their expertise. The diversity of the scopes of the involved organisations helped improve the Survey. Once all parties agreed on the Survey layout and questions, it was finalised to proceed with the following step.

Step 4 – Deployment and data collection

This survey step includes distributing the survey questions using the previously decided method. If the survey is online, the link for the survey should be shared with the relevant groups of people via social media, email, or other ways of online communication. Response data should be collected until the agreed cut-off date and stored for analysis at the next stage. In the case of online surveys, if any patterns show that respondents are leaving the survey incomplete at certain sections, it might indicate that it is not well designed and needs improvement. The purpose should be to have the maximum number of complete responses without compromising the cohesiveness and purpose of the survey.

This Survey employed the online survey platform Qualtrics. Therefore, the questions were transferred to Qualtrics in the agreed layout and checked by the involved organisations (Freshfields Bruckhaus Deringer, Accuracy, and NYUAD) before distribution. To protect the privacy of the respondents, IP addresses, location data, and contact information were anonymised by default. The respondents provided their contact information, which was kept confidential, in the last section of the Survey, if they wanted to receive the initial findings. Once the Survey was finalised, the link was shared with the partner organisations and via social media, such as LinkedIn. Some entities that received the Survey are the Society of Construction Law (SCL) Gulf and the Royal Institution of Chartered Surveyors (RICS). The distribution of the Survey started on 3 October 2022, and it was kept open until 31 December 2022 (90 days). While 187 people began the Survey during this period, 52 completed all sections.

Step 5 – Analysis and reporting

This is the last stage of a survey process. It includes analysing and interpreting the collected data and gathering the findings in a report to share them.

The responses to the questions were analysed to draw conclusions addressing the purpose of the Survey. While some findings were as expected, such as the high level of concern about cybercrime and low level of cybersecurity awareness and preparedness among project participants, some were unexpected. For example, only 15% of the respondents reported a significant increase in the vulnerability of their businesses to cybercrime due to the new working environment after COVID-19. The findings of the Survey, the main conclusions, and the recommendations to improve the security level of construction project participants are included in this report.

Conclusion

Our findings from the Survey highlight the vulnerability of construction businesses to cyber threats. Research supports the notion that cyberattacks are rising globally, and the construction sector is no exception. We do not consider this trend to be limited to the past. As the industry continues transitioning from paper-based record-keeping to more effective data management in electronic repositories, we expect a continued increase in cybersecurity threats to the sector. This mirrors the concerns expressed by 75% of respondents who feel there are cybersecurity issues in the construction sector.

The Survey results indicate that, while some project participants are aware of the importance of cybersecurity, there is a need for increased investment and education in this area. Only half of the respondents feel that their companies have significant or sufficient cybersecurity measures in place to protect against cyber threats in an environment where cybercrime targeted at the sector is rising rapidly. This finding is consistent with other studies, which suggest that many project participants lack the necessary cybersecurity measures and resources to protect themselves adequately from cyber threats.

Project participants must prioritise cybersecurity education, resources, and policy implementation at all levels of their business to address this issue. This need is magnified by the vast quantities of sensitive data that project participants are likely to hold. This approach aligns with recommendations made by cybersecurity experts, who suggest that project participants adopt a multi-layered approach to cybersecurity, including employee training, technology, and policy implementation. Additionally, working with cybersecurity and cybercrime experts can help project participants stay up-to-date on the latest cyber threats and implement appropriate measures to mitigate risks.

While the Survey primarily focused on insights from senior-level construction sector employees, it is essential to recognise that there might be variations in cyber awareness and understanding at different levels within a company. For instance, frontline workers or employees in administrative roles may have limited exposure to cybersecurity training or may not be fully aware of the potential risks and best practices. By contrast, IT professionals or those directly involved in technology implementation may have a higher understanding and familiarity with cybersecurity measures than employees in non-technical roles.

To gain a comprehensive understanding of the cybersecurity landscape within the construction sector, future research efforts could include a more comprehensive sample size, encompassing employees from various levels and departments. This would help capture a more diverse range of perspectives and potential disparities in awareness, as well as identify gaps in cybersecurity knowledge.

In summary, the Survey results emphasise the need for project participants to prioritise cybersecurity matters and implement appropriate measures to protect their networks, devices, and sensitive data from cyber threats. The rise of cybercrime in the construction sector is a growing concern, and project participants must take proactive steps to safeguard their assets and reputations. By working with cybercrime and cybersecurity experts and implementing comprehensive security measures, project participants can mitigate the risk of cyberattacks and protect themselves and their business partners from potential harm.

Contents
Introduction
Executive Summary
Findings
Recommendation
Methodology
Conclusion

freshfields.com

This material is provided by the international law firm Freshfields Bruckhaus Deringer LLP (a limited liability partnership organised under the laws of England and Wales authorised and regulated by the Solicitors Regulation Authority (SRA no. 484861)) and associated entities and undertakings carrying on business under, or including, the name Freshfields Bruckhaus Deringer in a number of jurisdictions, together referred to in the material as 'Freshfields'. For further regulatory information please refer to www.freshfields.com/support/legal-notice.

Freshfields Bruckhaus Deringer has offices in Austria, Bahrain, Belgium, China, England, France, Germany, Hong Kong, Ireland, Italy, Japan, the Netherlands, Singapore, Spain, the United Arab Emirates, the United States and Vietnam.

This material is for general information only and is not intended to provide legal advice.

© Freshfields Bruckhaus Deringer LLP 2024, January 2024, DS176531