Impacts of the Covid-19 Pandemic on Online Security Behavior within the UK Educational Industry.

Mololuwa Arogbodo
Department of Computing and informatics.
Bournemouth University
Dorset, United Kingdom
s5327994@bournemouth.ac.uk

***Abstract*— The emergence of the Covid19 pandemic has caused the shutdown of university activities on campus in the UK. There has been a migration of learning, teaching and assessment (LTA) into online virtual environments. This in turn resulted in a spike in cyber-attacks across educational businesses, as they seemed more vulnerable due to inadequate security systems that would facilitate online learning. In this research, the impact of the corona virus pandemic on the security behavior of academic businesses is uncovered. This is done by comparing the pre-pandemic annual cyber security survey with the peak and post-pandemic survey, i.e., 2019, 2020 and 2021 respectively. Findings from this research demonstrate that the pandemic brought about a rise in cyber-attack, which made universities prioritize security, and add defensive measures to ease online learning. Overall, the post-pandemic statistics suggests that educational businesses have improved their systems with adequate security measures, which makes the migration to online learning safe. That said, cyber attackers are innovative and will continue to impose a threat to these institutions. Therefore, improving security systems is a continuous process even when the pandemic put under control significantly or even eradicated.**

Keywords—Online Security behavior; Cyber Security; Cyberpsychology; Education; COVID-19 Pandemic)

I. INTRODUCTION

Following the declaration of the Covid-19 pandemic in the UK [1], the Government enforced a lockdown which meant that employees had to work from home. During this period, the cyber-crime rate increased by 400% [2], so much so that Covid-19 was classed as the biggest ever cyber security threat at the time [3]. Educational institutions had to carry out their lectures and meetings through virtual environments such as Zoom, Microsoft Teams, etc. [4][5]. This made universities an easy target for cyber criminals, as they were considered more vulnerable because school activities that would traditionally be held on campus, were online [6]. Amongst other forms of attack, E-mail Phishing attack was regarded as the most common attack during the lockdown [7]. This occurs when cyber criminals deceitfully try to gain access to unauthorized data (usually passwords and credit card details), by posing to be a trustworthy entity through E-mail [8]. In office settings, the established secure networks provide a layer of security that would prevent malicious emails from reaching employees, however, since these activities were being held online on personal networks without proper preparations, the risks to such entities are amplified.

Most universities hold an extensive volume of research data and innovative project ideas, that has been developed by students and staff within the university [9]. A successful cyber-attack compromises the confidentiality and integrity of such information as cyber criminals aim to steal and sell it. Furthermore, the damage to the reputation of the school organization is significant [10]. University's data contain financial records of students which are meant to be confidential. Access to such records makes parents lose confidence in the schools' ability to keep their financial information secure. The financial effects of these cyber-attacks are not overlooked. In 2020, Educational institutions spent over $2.5 million on recovering downtime, repairs, and lost opportunities due to cyber-attack [6]. In another report, educational organizations suffered 8 attacks on their Domain Name System (DNS) in 2020 and each attack cost over $850,000 [11].

The shift to online learning during the lockdown was meant to be a temporal solution, depending on the level of the pandemic and its eradication. However, the pandemic still exists and Universities can only offer a hybrid learning solution at best, combining both campus learning and online teaching when necessary. That said, this research aims to investigate the online behavior of educational institutions following the peak-pandemic period, which involves analyzing the current security measures put in place following the pandemic. To achieve the stated aim, previously published papers will first be examined to identify the security impact of the global pandemic in other sectors. Previous research concerned with analyzing cyber security risks in higher education will also be examined.

Research Questions: *(i) Has the Pandemic contributed to improving security awareness across academic institutions? (ii) Is the UK Education Sector now well equipped to fully migrate to online learning in the event of another pandemic?*

Paper Structure: *Section 2* discusses relevant literature with impact of the pandemic on security in other sectors. An overview of the threat land scape is uncovered in *section 3*. This would highlight various events of cyber breaches resulting from the lockdown. *Section 4* contains the analysis of the secondary research and comparisons. Its findings in *section 5*, will provide answers to research questions. The recommendations, limitations and guide for future research is discussed in *sections 6, 7 and 8* respectively.

II. Literature Review

The UK is amongst the list of countries most affected by the Covid-19 pandemic in terms of the volume of cases, as well as the length of its lockdown [2]. During the lockdown, employees across multiple industries had to embrace the work-from-home model (WFM). Most of these employees commonly reported challenges linked with the use of technology [12], and facing issues that on-site security networks would have eradicated.

Healthcare organisations has been one of the most vulnerable sectors to cyber-attacks resulting from the pandemic. According to the National Cyber Security Centre (NCSC), the UK health sector suffered an average of 60 cyberattacks per month between September 2019 and August 2020 (peak pandemic) [7]. The pandemic has made healthcare agencies adopt security measures that would protect patient information and data. Some of these measures include the use of Virtual Private Network (VPN), Enabling multi-factor authentication (MFA), constant updates of work systems, segmentation and separation of networks, etc [13].

Similarly, the financial sector was a big target for cyber criminals during the lockdown, the industry suffered a 38% rise in cyber-attack [14]. The financial services information sharing and analysis centre (FSISC) identified over 1,500 high-risk domains likely to have been established by threat actors, with these domains containing both financial and a Covid-19 theme [15]. That said, the financial industry has responded well during these times. They have adopted adequate security principles that mitigate the risk of being compromised. These principles include; proper software/application patches, raising awareness amongst employees, adequate incidence response plan, etc.

Relating to the educational sector, a paper by Ulven and Wangen conducts a systematic review of information security risks in higher education. The paper explains the threat actors, risks and vulnerabilities educational institutions face in the context of data security [16]. The paper also notes a scarcity of information and research on the analysis of cyber security in higher education. Given that this paper was published before the pandemic, the shift to online learning means the identified risks are heightened.

In another paper that focused on the issues presented in schools within the sudden change to online learning, its findings show that educational institutions experience issues due to their rapid transition to online learning and use of digital pedagogies. The paper concludes that the shift to online learning has resulted in dysfunctionality in delivering learning services, which some of the issues includes loss of service, denial of service, etc. [17].

III. Threat Landscape Of Vulnerabilities in the UK Educational Sector.

Educational businesses have a wide horizon of assets due to the diversity within the institution. They collect sensitive information from trustees, students, alumni, parents, faculty, staff, etc. [18]. These assets along with vulnerabilities resulting from the WFH model, makes cyber criminals target universities.

Oxford University, one of the top 3 Universities in the world [19], was a victim of a cyber-attack during the lockdown. Hackers gained access to their biochemical labs that had information on the Covid-19 vaccination at the time. This altered the progress of the research as their network had to be shut down due to the compromise [20].

Similarly, the University of Hertfordshire and the University of Northampton suffered attacks that disrupted their IT networks for days [21] [22]. Students and staff were unable to access Brightspace portals, and all academic activities were halted.

The threat actors responsible for attacks in this sector range from state-sponsored groups to steal information, to a curious white-hart hacker [16]. Different threat actors have multiple tactics used to exploit vulnerabilities. NCSC identified remote access systems as the common technique during the lockdown [7]. They use this system to exploit weak passwords, an absence of Multi-Factor Authentication (MFA), and a lack of regular updates to software. Also, attackers use social engineering techniques to take advantage of a lack of awareness in higher education [16]. Other common techniques include phishing, privilege escalation, Denial of Service (DoS), etc. Most of these techniques exploit the insufficient investment and management in cyber security within schools and colleges.

IV. Methodology and Findings

For this research, secondary data gotten from an annual survey conducted by the UK government's National Cyber Security Program will be used. This survey is usually aimed at uncovering the status of cyber security across various sectors in the UK.

The pandemic started in 2019, and has lasted ever since. Therefore, the educational survey Annex of 2019, 2020 and 2021 would be discussed.

a. Educational Survey Annex 2019 (Pre-Pandemic)

Educational institutions are known to hold a vast amount (76%) of personal data of their users (staff, students, parents), which are targets for cyber criminals. Senior managers in this industry say they prioritize cyber security, and they invest an average of **£7,000** per year. In 2019, **76%** of Educational Businesses admit they are likely to perform risk management actions, whilst also noting that about **42%** of its staff are aware of the importance of cyber security and online behaviour. About half **(50%)** of businesses that deliver educational services have dedicated departments for cyber security, and under **60%** of learning institutions have a proper cyber security policy in place [23].

b. Educational Survey Annex 2020 (Peak-Pandemic)

As earlier discussed, the pandemic and its induced lockdown amplified the risks educational institutions were exposed to, especially due to the WFH model across the country. During this period, **80%** of higher education identified cyber-attacks over the pandemic period, with **54%** saying they experienced an attack every week. Amongst these breaches, 57% suffered a material loss ranging from monetary value to loss of data and network. This led to **82%** of the victims requiring new security measures following the breach. It is worth noting that the high percentage of victims who needed new security measures, signifies that the previous security measures and policy were not adequate enough to mitigate the risks faced during the pandemic.

Similar to 2019, over 90% of senior managers prioritize cyber security and require regular updates on the status of their cyber security vulnerability. That said, there is a significant difference in the percentage of educational businesses with cyber security policy in 2020 (97%) compared to the previous year **(57%).** Also, there are more educational businesses with trustees dedicated to cyber security at over **70%** this year, compared to **50%** in 2019 [24]. Recognizing the growing importance of cyber security at the time, 51% of academic institutions insured themselves against cyber security risks.

c. Educational Survey Annex 2021 (Post-Pandemic)

Health responders committed time and resources towards eradicating the Covid-19 pandemic, and it substantially reduced in 2021. Schools began to open to student, albeit providing a hybrid structure of learning with lectures and meetings sometimes on-site and other times online. In 2021, **75%** of UK universities identified cyber security breaches with **26%** claiming they suffered a breach every week, a slightly lower figure compared to 2020's **80%** and **54%** respectively. During this period, 33% of educational institutions suffered material losses amongst which **58%** of them needed new security measures to be installed. Like previous years, **95%** of senior managers prioritize cyber security and require updates regularly. Also, about **70%** of educational businesses have trustees dedicated to cyber security within the firm. There is a **10%** increase in the value of staffs trained on the importance of cyber security in the industry. Similar to 2020, there is a high number of learning institutions with cyber security policies and adequate incidence response plan [25].

V. Observations and Discussions

Based on the statistical analysis illustrated in this research, most educational institutions had the adequate security measures and policies on-site to counter cyber attackers. Although Universities already used online remote services and security monitoring tools for remote work, the spike in security breaches identified in 2020 suggests that these institutions were not prepared for the full shift towards the WFH model, hence the risks they were exposed to were amplified. In 2021, it is observed that there is conscious attention towards cyber security within the educational sector. It is worth noting that educational businesses emphasized on the use of new technology during this period. They particularly noted the emergence of VPN software that protects networks from cyber criminals. Alongside the use of secure VPN software, they have also adopted the use of multi-factor authentication across all the online portals for both students and staffs of the organization. The 2021 statistics is evidence that the new measures introduced due to the spike in previous has contributed to minimizing the vulnerabilities in this sector. The Covid-19 pandemic ensured that presidents of educational organizations invested more in the cyber security, spending more in three months almost what they would have traditionally spent in two years [7].

The summary of results from the survey comparing 2020 results with 2021 is illustrated in table 1 below;

	2020	2021
Attacks suffered	80%	75%
Material loss suffered	57%	33%
Attacks per week	54%	26%
Risk Management	60%	40%
Trustees responsible for security	70%	66%
Awareness amongst staff	46%	56%
Policies regarding security	70%	86%

Table 1. Summary of Results (Source: Author)

VI. Recommendations

The pandemic has made management in schools pay more attention to cyber security, and has resulted in monetary investment to secure data on their networks. Academic institutions within the UK are on the right path towards improving their security systems. That said, the pandemic is not going to last forever, and cyber attackers are constantly discovering new ways of gaining unauthorized access to sensitive data. To avoid complacency and ensure the efforts of attackers remain void, the following recommendations are made:

a. Regular Risk Assessment

Effective quantitative and qualitative risk assessments should be conducted regularly to ensure that adequate security measures are in place to minimize risk to a level acceptable to the management of educational businesses [26].

b. Frequent Security Awareness schemes.

Universities and colleges experience a constant influx of students and staff each year, and they all need to be aware about the importance of maintaining safe online behavior to avoid a breach. It is also necessary to update existing students and staff on the expected security behavior, so as to prevent complacency amongst them.

c. Defined Security Policy and Investments to Security.

Security policies need to be set in educational environments to guide students and staff on maintaining safe online behavior [27]. The policy should contain strict rules and penalties where applicable. This would help keep members of the academic community in check, and contribute to ensuring safe security systems.

Adequate investment should be made in security departments in terms of laour (quantity of staff) and finance. This would ensure that software systems are updated and properly patched.

VII. Limitations

a. Bias.

The use of surveys/questionnaires rather than measuring direct security architectures in place may limit the validity of the findings. Participants of a survey answer questions with a level of bias in order to look positive and preserve reputation, despite the assurance of anonymity.

b. Scalability and Volume of Data.

For accurate statistical interpretation of data, the number of users being evaluated has to be substantial. The volume of users surveyed for this research is too small to be statistically reliable. 135 primary schools were surveyed, along with 158 secondary schools and 57 colleges. However, the number of higher education institutions within the UK is very small and as such, the results from a survey of this size can provide a good estimation and indication of where the educational sector stands in its cyber security measures.

VIII. Conclusion and Future Work

This research focused on comparing the annual survey conducted in 2019, 2020 and 2021 to assess the impact of the pandemic in the UK Educational sector. This is because the number of empirical studies concerned with information security in academic institutions is quite limited. Future research should conduct its research as a source of primary data (following all ethical procedures), and present its own findings which would either validate or reject the findings from this research.

Furthermore, the identified recommendations from this research can be looked into and discussed into detail. Methods on how to raise awareness in academic environments, and the role of psychology towards achieving awareness of students and staff should be discussed.

One of the issues faced amongst the victims of cyber-attack during the pandemic is the unavailability of a proper incident response plan. Future research should focus on designing a framework for Academic Businesses, that would improve the incident response of such businesses, so as to mitigate the identified risks.

IX. References

[1] WHO, "Coronavirus Disease (COVID-19) - Events as They Happen," *www.who.int*, Jul. 31, 2020. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

[2] J. Deutrom, V. Katos, and R. Ali, "Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19," *Behaviour & Information Technology*, pp. 1–15, Sep. 2021, doi: 10.1080/0144929x.2021.1973107.

[3] P. Security, "43 COVID-19 Cybersecurity Statistics," *Panda Security Mediacenter*, Aug. 26, 2020. https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/.

[4] M. Babinčáková and P. Bernard, "Online Experimentation during COVID-19 Secondary School Closures: Teaching Methods and Student Perceptions," *Journal of Chemical Education*, vol. 97, no. 9, pp. 3295–3300, Aug. 2020, doi: 10.1021/acs.jchemed.0c00748.

[5] H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *Computers & Security*, vol. 105, p. 102248, Mar. 2021, doi: 10.1016/j.cose.2021.102248.

[6] N. Kshetri, "Cybercriminals use pandemic to attack schools and colleges," *The Conversation*, Sep. 25, 2021. https://theconversation.com/cybercriminals-use-pandemic-to-attack-schools-and-colleges-167619.

[7] National Cyber Security Centre, "NCSC defends UK from more than 700 cyber-attacks while supporting national pandemic response," *www.ncsc.gov.uk*, Nov. 03, 2020. https://www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic.

[8] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A Survey of Phishing Email Filtering Techniques," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013, doi: 10.1109/surv.2013.030713.00020.

[9] A. Townsend, "3 reasons higher education is attractive to hackers," *OneLogin*, Feb. 26, 2021. https://www.onelogin.com/blog/3-reasons-higher-ed-hacked.

[10] S. Campbell, "Cybersecurity in Higher Education: Problems and Solutions," *Toptal Insights Blog*, 2018. https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education.

[11] EfficientIP, "Mitigating Data Theft in the Education Sector with DNS Security," *EfficientIP*, Sep. 03, 2020. https://www.efficientip.com/data-theft-education-dns-security/ (accessed Jan. 06, 2022).

[12] Z. R.Alashhab, M. Anbar, M. Singh, Y.-B. Leau, Z. Al-Sai, and S. Alhaja'a, "Impact of coronavirus pandemic crisis on technologies and cloud computing applications," *Journal of Electronic Science and Technology*, p. 100059, Nov. 2020, doi: 10.1016/j.jnlest.2020.100059.

[13] B. Pranggono and A. Arabo, "COVID -19 Pandemic Cybersecurity Issues," *Internet Technology Letters*, vol. 4, no. 2, Oct. 2020, doi: 10.1002/itl2.247.

[14] J. Crisanto and J. Prenio, "FSI Briefs No 7 Financial crime in times of Covid-19 - AML and cyber resilience measures," 2020. [Online]. Available: https://www.bis.org/fsi/fsibriefs7.pdf.

[15] Financial Services Information Sharing Centre, "High Risk Domains with a COVID-19 and Financial Theme," 2020. Accessed: Nov. 09, 2021. [Online]. Available: https://www.fsisac.com/hubfs/Resources/FSISAC-HighRiskDomains-COVID19Theme-TLPWhite.pdf.

[16] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," *Future Internet*, vol. 13, no. 2, p. 39, Feb. 2021, doi: 10.3390/fi13020039.

[17] M. M. Zalat, M. S. Hamed, and S. A. Bolbol, "The experiences, challenges, and acceptance of e-learning as a tool for teaching during the COVID-19 pandemic among university medical staff," *PLOS ONE*, vol. 16, no. 3, p. e0248758, Mar. 2021, doi: 10.1371/journal.pone.0248758.

[18] J. Giszczak and D. Paluzzi, "Pass or Fail? Data Privacy and Cybersecurity Risks in Higher Education | Martindale.com," *www.martindale.com*, Sep. 12, 2016. https://www.martindale.com/legal-news/article_mcdonald-hopkins-llc_2234700.htm (accessed Jan. 10, 2022).

[19] Times Higher Education, "World University Rankings," *Times Higher Education (THE)*, Aug. 25, 2021. https://www.timeshighereducation.com/world-university-rankings/2022/world-ranking#.

[20] S. Morrison, "Oxford University coronavirus research lab targeted in cyber attack," *www.standard.co.uk*, Feb. 25, 2021. https://www.standard.co.uk/news/uk/hackers-oxford-university-coronavirus-research-lab-cyber-attack-b921297.html (accessed Jan. 10, 2022).

[21] J. Coker, "Uni of Hertfordshire Suffers Cyber-Attack That Takes Down its Entire IT Network," *Infosecurity Magazine*, Apr. 15, 2021. https://www.infosecurity-magazine.com/news/uni-hertfordshire-cyber-attack-it/ (accessed Jan. 10, 2022).

[22] Z. Marzouk, "University of Hertfordshire's entire IT system offline after cyber attack," *IT PRO*, Apr. 15, 2021. https://www.itpro.co.uk/security/cyber-attacks/359222/university-of-hertfordshire-hit-by-cyber-attack.

[23] Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2019," *GOV.UK*, Apr. 03, 2019. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.

[24] Department for Digital, Culture, Media & Sport, "Cyber Security Breaches Survey 2020," *Computer Fraud & Security*, vol. 2020, no. 4, p. 4, Apr. 2020, doi: 10.1016/s1361-3723(20)30037-3.

[25] Department for Digital, Culture, Media & Sport, "DCMS: Cyber Security Breaches Survey 2021," *Network Security*, vol. 2021, no. 4, p. 4, Apr. 2021, doi: 10.1016/s1353-4858(21)00036-2.

[26] National Cyber Security Centre, "Alert: Further ransomware attacks on the UK education sector by cyber criminals," *www.ncsc.gov.uk*, Jun. 04, 2021. https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector#section_6 (accessed Jan. 11, 2022).

[27] B. Violino, "How to Protect Distance Learning Against Cyber Threats," *businessinsights.bitdefender.com*, Nov. 17, 2021. https://businessinsights.bitdefender.com/how-to-protect-distance-learning-against-cyber-threats (accessed Jan. 11, 2022).