**The nature of cyber threats has changed dramatically over the past three decades**

Word Count -1,865

# Abstract

Cyber-attacks undeniably evolve over time since indoctrination of the internet, new technology and practices. This report evaluates examples of cyber-attacks over the past three decades and beyond, how they have evolved over time to present day, as well as problems faced within security management previously in conjunction with the next decade. Additionally, literature reviews are conducted on disparate sources to research related information determining such possibilities. Current findings indicate whilst a proportion of cyber-attacks are better handled currently compared to history, others are still widespread now and going forward; and with new technology arises new threats and complexities to deal with. Furthermore, cyberattacks related to social engineering will likely still prevail in the future. Finally, current legislation will not be fungible for the technological future; both the further emergence of Internet of Things, and introduction of Quantum Computing dramatically changes the landscape for security management practices.

**Keywords—Cyber-attack, Technology, Internet of Things, Social Engineering, Quantum Computing.**

# Introduction

Cyber-attacks presently define as forms of cybercrime relating to illegal activity, where attacks target individuals and organisations alike; attempting to access sensitive information, compromise technology resources, from a criminal, political or personal impetus [1, p. 62], [2-4]. These attacks create fundamental issues in using technology, from hijacking information, or causing strains on resource for organisations and public alike; facing these threats when interactions occur over a network synergising with technology and internet. Therefore, this report considers forms and mutations of cyberattacks over three decades experienced by average users; including threats emerging exposed new technology in open and commercial spaces in the next decade. The report also speculates issues faced from multiple perspectives that could arise from new threats and technology.

# Cyber-attack mutation over time

An early example of a cyber-attack, could reach as far back as the late 1970’s – 1990’s as stated by Middleton [5, pp. 6–10] Where Kevin Mitnick gained unauthorised access to computer networks, by hacking – attempts to breach or access systems [6, p. 32], [7, pp. 93–94], [8, pp. 21–22], [9, p. 69], including use of social engineering - influencing people to provide sensitive information or access [10, p. 63], [11, p. 5], [12]. Furthermore, these types of attacks are still prevalent in Information Security (IS) and Risk Management today, where social engineering has evolved further. A later example recorded in 2013 by Johnson [13] quoted further in studies [14-15] demonstrates social engineering performed on an individual who received a malicious email to process an invoice, with an impersonator masquerading an official, calling to persuade them to process said invoice, which was in fact malicious code. This scenario uses social engineering derivatives such as Pretexting and Vishing – for someone to comply to an impersonator’s instructions [16, p. 7], [17]. Whilst the concept remains close to the previous example, the method or technique has become far more sophisticated and still involves human elements; Thus, provides challenges mitigating from this form of cyber-attack, as people are deemed the most error prone and manipulatable, without updated guidance and training [10, p. 63], [22, pp. 3–4].

Another evolving cyber-attack seen, becoming more complex presently involves computer viruses. One instance derives from an event in 1974 with introduction of the Wabbit Virus; a self-replicating worm to reduce or stop system performance of a computer – also known as a fork bomb [18-19]. Since then, evolution has occurred to another version of malware known as denial of service (DoS) attacks, preventing use of a network, to flooding the resource with unnecessary traffic, which a Distributed Denial of Service (DDoS) can flood from multiple sources. [9, p. 69], [20, p. 5]. An example in recent times has been recorded in Q1 2020 by Amazon where Amazon Web Services (AWS)were affected on a grand scale of over 300,000 DDoS attacks with a maximum bit rate attempting to transfer of 2.3 Terabytes [21].

In the past three decades and beyond, it can be seen from examples above how these cyber-attacks within their and technologies infancy, has grown substantially, becoming more complex and multifaceted, which creates new challenges to mitigate these types on an ongoing basis; and could continue to grow and adapt as technology does, which theories are presented in the section based on how technology - with associated cyber-attack risk – potentially advancing in the next decade.

# Challenges facing the next decade of technological advancement

As seen from above, one could argue that as technology evolves over time, as does the types of cyber-attacks facing an organisation or public alike. It is suggested the not-so-distant future will bring about the Technological Singularity; where Tzezna and Newitz [23-24] describe as a set of ground-breaking technologies, which completely changes people’s lives to the point of no return. Furthermore, Zola [25] describes it as a hypothetical future where growth in technology drastically transforms reality as we deem it to be at present, where a post-singularity world is unrecognisable. Considering above, there are several emerging and evolving technologies that challenges will be faced.

## Internet of Things (IOT)

IOT described by Shancang, Li Da and Shanshan [26], as using devices connected over a network via the use of sensors. Further explained by Kumar, Tiwari, and Zymbler [27] where the introduction of smart devices provides solutions to day-to-day challenges. Whilst this technology is still relatively newly adopted todayt, there are still risks faced with using such a technology that needs to manage to prevent issues. Such raised challenges raised in the following paper [28] still include vulnerabilities to DoS attacks and ensuring secure data transfer and authentication to name a few. These challenges are highlighted further by Chacko and Hayajneh [29] stating where IoT has been beneficial for the treatment of patients, security and privacy concerns are still prevalent such as DDoS attacks secure protection of patient’s data, especially with a new form of attack known as Medjacking – the practice of hacking a medical device with harmful intent towards a provider or patient [30-33].

## Quantum Computing

Wong [34] defines quantum computing as the use of qubits – basis states with superposition – to perform calculations on multiple basis states at the same time, where logic gates are reversible, which is not replicated in modern computing today. Due to the nature of how quantum computing operates compared with classical computing, it poses new challenges and risks not anticipated thus far. One form of risk documented is the current use of cryptography - providing secure encryption to classical computers to secure communication using cyphers, ensuring security using mathematical concepts [35, p. 44], [36]. However, quantum computing will make current encryption techniques obsolete. As stated by Costello [37] whereby quantum computers will break all encryption currently used as protection from hackers. However, Sharma [38] argues that cyber attacks from quantum computing, could be defended against via quantum computing and quantum physics, including true random number generators that could be applied to classical computers. Based on above, whilst there some potential for quantum computing to be both useful and protected against, there seems little protection and substantial risk at present if a quantum computer would be used for malicious intent against current computing systems.

# Non-technological issues to arise in the next decade

As well as challenges faced in risk management with emergence and evolution of new technology and data practices over the next decade, there will be other perspectives which need consideration outside of a technological standpoint; this may include legal, ethical, professional, or political perspectives. From one viewpoint there will be similar issues faced in the current age that will continue to exist, as well as new complications that may arise in future.

## Ethical

One Issue already started, as well as continues further, is how technology is changing the way users and organisations perform activities. Examples quoted by El-Bahrawy [39] such as streaming and subscription services whilst convenient, users have no ownership and creates a vulnerability of loss if such a service loses access for a user, or the service stops. Furthermore, services and organisations taking invasive steps on users’ information and data, to confirm identity, including unintentional or malicious misuse of it. As implied by Berman [40] further information could be taken from users to further scrutinise any they come across. As security management is aiming to provide enhanced security checks of individuals, this may encroach risk to using features of users confirming their identity; such as protected characteristics corresponding race, gender, sexual orientation [41], or financial status; if not managed effectively, bias could be re-introduced discriminating users engaged such service, increased risk of breaching the Equality Act 2010 [42], as well as the very measure to reduce certain cyber-attacks, could actually induce others being opportunely.

.

## Legal

Legislation on security management is outpaced by evolution of technology advances and practices. As proposed by Marchant [43], legal processes lack significant oversight or speed needed due to ossification to keep pace with emerging technology; unless these methods alter to accommodate a more reactive or hopefully a proactive response to security management threats, legislation in security management will always be catching up after much time has passed. However, if the concept of counter-law mentioned by Molnar [44], explained further by Ericson [45] where legislation is established to erode previous principles. Whilst indicates negative connotations to previous use in aspects of counterterrorism, the concept of counter-law could be used in security management to keep closer at pace with new technological threats.

## Professional

First and foremost, the one issue from a professional perspective for maintaining security management in the next decade, will come down to compliance and training. As inevitably, as new technology is used in the next decade, so to will new and more complex cyber-attacks, with increasingly complex business environments to work within, managing the workload of employees to keep security management as effective as it can be, and potential widening of the skills gap for cyber-security roles and the amount of skill professionals to fill them [46-47]. Not only from compliance and training, but there will also be risk by not knowing where efforts should be placed when attempting to deal with new threats to security threats, as unless a type of cyber-attack has happened before, new types could emerge that are not yet known.

# Conclusion

Technology – and the management of it – will not cease to evolve in the advancement of society known now and in the future, and so too will the threats of cyber-attacks with and against it. This report examines instances of cyber-attacks over history, and how they evolved in recent times; provided a non-exhaustive selection of examples on challenges faced in technology over the next decade potentially, as well as the non-technological issues that could be seen with it. It is believed the use of social engineering based cyber-attacks will remain a threat in which to be vigilant of, for the foreseeable. Additionally, the further development of Internet of Things (IoT) and introduction of Quantum Computing will dramatically change the landscape of security management as currently known, where additional risk will be seen. Finally, current legislation will not be suitable for the next decade of security management, and the use of counter-law could be adopted, and rapid training of professionals are required ensuring security management can be implemented effectively as possible where new and unknown threats emerge.

# References

[1] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, p. 62.

[2] IBM, “What is a cyber attack? | IBM,” www.ibm.com. https://www.ibm.com/uk-en/topics/cyber-attack (accessed Jun. 02, 2022).

[3] NCSC, “How Cyber Attacks Work,” Ncsc.gov.uk, 2019. https://www.ncsc.gov.uk/information/how-cyber-attacks-work (accessed Jun. 02, 2022).

[4] Cisco, “Cyber Attack - What Are Common Cyberthreats?,” Cisco. https://www.cisco.com/c/en\_uk/products/security/common-cyberattacks.html (accessed Jun. 02, 2022).

[5] B. Middleton, A history of cyber security attacks : 1980 to present. Boca Raton, Fl: Crc Press, 2017, pp. 6–10.

[6] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, p. 32.

[7] K. D. Mitnick and W. L. Simon, The Art of Deception : Controlling the Human Element of Security. Hoboken; Indianapolis, Indiana: Wiley, 2002, pp. 93–94.

[8] W. Schmidt, Cissp: A Comprehensive Beginners Guide on the Information Systems Security. Independently Published, 2019, pp. 21–22.

[9] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, p. 69.

[10] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, p. 63.

[11] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, p. 5.

[12] K. D. Mitnick and W. L. Simon, The Art of Deception : Controlling the Human Element of Security. Hoboken; Indianapolis, Indiana: Wiley, 2002.

[13] A. L. Johnson, “Endpoint Protection - Symantec Enterprise,” community.broadcom.com, Aug. 28, 2013. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=e20ae74f-2fe9-42b2-a473-8affe234d050&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (accessed Jun. 02, 2022).

[14] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” 2014 Information Security for South Africa, Aug. 2014, doi: 10.1109/issa.2014.6950510.

[15] F. Mouton, L. Leenen, and H. S. Venter, “Social engineering attack examples, templates and scenarios,” Computers & Security, vol. 59, pp. 186–209, Jun. 2016, doi: 10.1016/j.cose.2016.03.004.

[16] K. D. Mitnick and W. L. Simon, The Art of Deception : Controlling the Human Element of Security. Hoboken; Indianapolis, Indiana: Wiley, 2002, p. 7.

[17] M. Security, “6 Types of Social Engineering Attacks,” www.mitnicksecurity.com, Apr. 05, 2021. https://www.mitnicksecurity.com/blog/6-types-of-social-engineering-attacks (accessed Jun. 02, 2022).

[18] D. Shah, V. Shah, H. Shah, and P. Kanani, “Survey on Computer Worms,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, no. 8, pp. 184–194, Aug. 2017, doi: https://doi.org/10.17762/ijritcc.v5i8.1190.

[19] B. Rajesh, Y. R. Janardhan Reddy, and B. Dillip Kumar Reddy, “A Survey Paper on Malicious Computer Worms,” International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015), vol. 3, no. 2, p. 162, 2015, Accessed: Jun. 02, 2022. [Online]. Available: http://www.ijarcst.com/doc/vol3issue2/ver2/brajesh.pdf

[20] Darril Gibson, Managing Risk In Information Systems. S.L.: Jones & Bartlett Learning, 2020, p. 5.

[21] Amazon, “AWS Shield Threat Landscape Report -Q 1 2020,” 2020. Accessed: Jun. 02, 2022. [Online]. Available: https://aws-shield-tlr.s3.amazonaws.com/2020-Q1\_AWS\_Shield\_TLR.pdf

[22] K. D. Mitnick and W. L. Simon, The Art of Deception : Controlling the Human Element of Security. Hoboken; Indianapolis, Indiana: Wiley, 2002, pp. 3–4.

[23] Roey Tzezana, “Singularity: Explain It to Me Like I’m 5-Years-Old,” Futurism, Mar. 03, 2017. https://futurism.com/singularity-explain-it-to-me-like-im-5-years-old (accessed Jun. 04, 2022).

[24] A. Newitz, “What Is The Singularity And Will You Live To See It?,” Gizmodo, May 10, 2010. https://gizmodo.com/what-is-the-singularity-and-will-you-live-to-see-it-5534848 (accessed Jun. 04, 2022).

[25] A. Zola, “What is the singularity?,” TechTarget, 2019. https://searchenterpriseai.techtarget.com/definition/Singularity-the (accessed Jun. 04, 2022).

[26] S. Li, L. D. Xu, and S. Zhao, “The internet of things: a survey,” Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, Apr. 2014, doi: 10.1007/s10796-014-9492-7.

[27] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” Journal of Big Data, vol. 6, no. 1, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[28] A. ur Rehman, S. ur Rehman, I. U. Khan, M. Moiz, and S. Hasan, “Security and Privacy Issues in IoT,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 8, no. 3, 2016, doi: 10.17762/ijcnis.v8i3.2074.

[29] A. Chacko and T. Hayajneh, “Security and Privacy Issues with IoT in Healthcare,” EAI Endorsed Transactions on Pervasive Health and Technology, vol. 4, no. 14, p. 155079, Jul. 2018, doi: 10.4108/eai.13-7-2018.155079.

[30] K. Breene, “What is medjacking?,” World Economic Forum, Oct. 20, 2016. https://www.weforum.org/agenda/2016/10/medjacking-health-cyber-risk-explainer/#:~:text=Medjacking%20 (accessed Jun. 04, 2022).

[31] Wikipedia, “Medical device hijack,” Wikipedia, Jan. 01, 2022. https://en.wikipedia.org/wiki/Medical\_device\_hijack (accessed Jan. 17, 2022).

[32] E. Y. Adashi and N. M. Thomasian, “Medical Devices in Harm’s Way: Medjacking,” JAMA Health Forum, vol. 1, no. 1, p. e200007, Jan. 2020, doi: 10.1001/jamahealthforum.2020.0007.

[33] S. Meggit, “MEDJACK Attacks: The Scariest Part of the Hospital,” Tufts University, Dec. 2018. Accessed: Jun. 04, 2022. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2018/smeggitt.pdf

[34] H. Y. Wong, INTRODUCTION TO QUANTUM COMPUTING : from a layperson to a programmer in 30 steps. S.L.: Springer Nature, 2022.

[35] W. Schmidt, Cissp: A Comprehensive Beginners Guide on the Information Systems Security. Independently Published, 2019, p. 44.

[36] GeeksforGeeks, “Cryptography and its Types - GeeksforGeeks,” GeeksforGeeks, Jul. 08, 2019. https://www.geeksforgeeks.org/cryptography-and-its-types/ (accessed Jun. 04, 2022).

[37] C. Costello, “Craig Costello: In the war for information, will quantum computers defeat cryptographers? | TED Talk,” www.ted.com. May 2019. Accessed: Jun. 04, 2022. [Website Video]. Available: https://www.ted.com/talks/craig\_costello\_in\_the\_war\_for\_information\_will\_quantum\_computers\_defeat\_cryptographers?subtitle=en

[38] V. Sharma, “How quantum physics can make encryption stronger,” www.ted.com. Dec. 2017. Accessed: Jun. 04, 2022. [Online]. Available: https://www.ted.com/talks/vikram\_sharma\_how\_quantum\_physics\_can\_make\_encryption\_stronger?subtitle=en

[39] S. El-Bahrawy, GCSE AQA computer science for the grade 9-1 course : the revision guide. Broughton-In-Furness? Cgp Books, 2018, pp. 66–67.

[40] J. J. Berman, Principles and practice of big data preparing, sharing, and analyzing complex information. London Cambridge, Ma Academic Press, An Imprint Of Elsevier, 2018, pp. 419–420.

[41] GOV.UK, “Discrimination: your rights,” GOV.UK, 2010. https://www.gov.uk/discrimination-your-rights (accessed Jun. 17, 2022).

[42] GOV.UK, “Equality Act 2010,” Legislation.gov.uk, 2010. https://www.legislation.gov.uk/ukpga/2010/15/contents (accessed Jun. 17, 2022).

[43] G. E. Marchant, “The Growing Gap Between Emerging Technologies and the Law,” The International Library of Ethics, Law and Technology, vol. 7, pp. 19–33, 2011, doi: 10.1007/978-94-007-1356-7\_2.

[44] A. Molnar, “Technology, Law, and the Formation of (il)Liberal Democracy?,” Surveillance & Society, vol. 15, no. 3/4, pp. 381–388, Aug. 2017, doi: 10.24908/ss.v15i3/4.6645.

[45] R. Ericson, “Security, surveillance and counter-law,” Criminal Justice Matters, vol. 68, no. 1, pp. 6–7, Jun. 2007, doi: 10.1080/09627250708553271.

[46] W. Erstad, “9 Cyber Security Problems Nearly Every Organization Struggles With,” Rasmussen.edu, 2019. https://www.rasmussen.edu/degrees/technology/blog/cyber-security-problems/ (accessed Jun. 17, 2022).

[47] A. Subhani, “Council Post: Emerging Challenges For Information Security Professionals,” Forbes, Aug. 20, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/08/20/emerging-challenges-for-information-security-professionals/?sh=36f70df81434 (accessed Jun. 17, 2022).