The Context of Security Within the Fourth Industrial Revolution

Anthony Caldwell
Axway, Ireland

Abstract

The fourth industrial revolution is characterized by cyber-physical systems, where technology becomes more embedded within society. Within this context, the risk associated with trust in this digital transformation is a critical relationship. The prevalence of cyber-attacks which have disrupted critical infrastructures have led to the emerging perception that active defenses are becoming appropriate. Security by design is increasingly leveraged into the early phases of product development right up to product release. Enhancing the understanding of cybersecurity in digital transformation, the red team/blue team exercise as well as a consideration of the Internet of Things (IoT) are outlined.

1. Introduction

The growth and potential of digital transformation will have important impacts upon many economies worldwide, what some have characterized as a fourth industrial revolution. Early reports on the digital economy estimated at 22.5% of the world economy, shows the US being the world leaders in this respect having amassed USD 5.9 trillion (33% of its Gross Domestic Product (GDP)) rising to 2.1% of GDP in 2020, equivalent to additional USD 421 billion [1]. The impressive success of the digital economy comes fraught with risks as well as rewards. In this respect, a focus of intense interest surrounding the relevance of cybersecurity has penetrated into many areas of computer science, economics, AI and law to name a few. In today’s highly interconnected world, an increasingly wide variety of applications, ranging from small systems such as company internet and email filtering to larger scale complex, mission critical systems such as oil pipelines and hospital administration systems are now being subjected to security attacks. This paper introduces some of the important themes developing within the discussions on digital transformation through the lens of cybersecurity and highlights the danger of active defences and how security by design leverages the philosophy of security into the early software development life cycle.

2. The Fourth Industrial Revolution

The World Economic Forum (2016), characterizes the first industrial revolution as a shift from a dependence upon animals, human effort, and biomass as primary sources of energy to the use of fossil fuels and the mechanical power this enabled. The second industrial revolution from the 19th century and the first two decades of the 20th century, brought electricity, wireless and wired communication, medical advances in terms of vaccines and new forms of power generation. The third industrial revolution from the 1950s began the digital era of communications and advances in computing power. The fourth industrial revolution may be characterized by cyber-physical systems, where technology becomes more embedded within societies and even our human bodies [2], [3]. More broadly, given the distribution of wealth, ideas around inequality, security and identity are becoming the major themes which are defining the fourth industrial revolution, with cyberspace as the strategic a theatre of engagement [3]. Also known as Industry 4.0, the fourth industrial revolution, may also be characterized by the integration of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), and machine learning into traditional manufacturing and industrial practices. These technologies have the potential to revolutionize the way we live and work, bringing about significant improvements in productivity, efficiency, and accuracy. However, with the increasing reliance on technology also comes an increased risk of cybersecurity threats. In the context of Industry 4.0, cybersecurity is crucial for protecting sensitive data, intellectual property, and critical infrastructure. As more and more devices become connected to the internet, the attack surface for hackers and cybercriminals grows exponentially, making it harder to secure networks and systems. One of the major challenges of cybersecurity in Industry 4.0 is the sheer number and variety of connected devices. The IoT consists of billions of devices ranging from smart thermostats and security cameras to industrial control systems and medical devices. These devices often have limited computing power and are vulnerable to attacks due to their lack of strong security measures. Hackers can exploit vulnerabilities in these devices to gain access to a network and potentially compromise sensitive data or disrupt operations. Another challenge is the complexity of Industry 4.0 systems. Traditional manufacturing systems consist of isolated machines that are controlled by a central computer. In contrast, Industry 4.0 systems involve a network of interconnected devices that communicate and exchange data in real-time. This creates a complex web of connections that can be difficult to secure and monitor. Hackers can potentially exploit these connections to gain access to a network and disrupt operations. To address these challenges, organizations must adopt a robust cybersecurity strategy that includes both technical and non-technical measures. On the technical side, this may involve implementing strong passwords, two-factor authentication, and encryption to protect data and secure communication. It may also involve regularly updating software and installing security patches to address vulnerabilities. On the non-technical side, organizations must educate employees on cybersecurity best practices and establish policies and procedures to ensure that everyone is following safe and secure practices. Cybersecurity is a crucial consideration in the context of Industry 4.0. With the integration of advanced technologies and the increasing reliance on the internet, the risk of cyber threats has grown significantly. To protect against these threats, organiz -ations must adopt a comprehensive cyber security strategy that includes both technical and non-technical measures. By taking these steps, we can ensure that the benefits of Industry 4.0 can be realized while minimizing the risk of cyber-attacks. The digital transformation paradigm for developing software applications, characterized by the merging of technology and economy, while facilitating and transforming business transactions to access new markets, has highlighted some of the security risks associated and importantly, in many economies worldwide has emphasized the significance of trust.

3. The Importance of Trust

Trust is the foundation of commerce. As noted by Teo and Mahmood [4] the rise of the digital economy obviates the need for secured cyberspaces in which to do business. Indeed, cyber threats have been and most likely will be an aspect of doing business that we continually mitigate for [5], [6]. From a nation state perspective, a crucial element in national security standards is the difficult balance between the needs of the economy with the security of the cyberspace in which it operates [7]. Indeed, defence against cyber threats has become an ever-increasing priority for nations across the globe. In 2015, UK government classified cyber threats as the principal risk in their 2015 National Security Strategy (NSS). Similarly, in the US, released the Department of Defence Cyber Strategy in 2015. National cybersecurity focusses on critical infrastructure protection in order to effectively combat cybercrime and strengthen national defence capabilities [8[, [9], [10]. What drives its development is an intrinsic need for trust and security. As noted by Suh and Han (2003), trust is based on previous interactions between supplier and purchaser, but previous behaviour does not guarantee that a supplier will act as expected and importantly, a customer's trust increases if the supplier does behave as previously expected [11]. This suggests that the risk associated with trust in digital transformation is a critical relationship and, more than ever, the relevance of cybersecurity in this relationship comes to the fore. For, anything unexpected that detrimentally affects consumers inevitably erodes public trust. It is here that the relevance of cybersecurity, not only in the technological sense but also in the reputational sense can mitigate for this erosion. Trust plays a crucial role in cybersecurity, as it is essential for building and maintaining secure relationships between individuals and organizations. Without trust, it is difficult to effectively collaborate and exchange information, which are important for maintaining the security of networks and systems. Trust is also important for building user confidence in the security of a system or service. In the context of cybersecurity, trust is often established through the use of secure authentication methods, such as passwords and two-factor authentication, as well as encryption, which helps to protect the confidentiality of sensitive information. Trust is also built through the responsible handling of personal data and the transparent communication of security measures and practices.

Maintaining trust in cybersecurity is important for both individuals and organizations, as it helps to ensure the security and integrity of systems and networks and helps to protect against cyber threats such as hacking and data breaches. In cybersecurity, risk is a function of the likelihood that a cybersecurity incident will occur and the impact that it can generate [12]. On this basis, cybersecurity approaches are in constant research and development because of the growing cyber threat attack landscape, a dangerous mix of state-based actors, cyber-criminal organizations and private sector components are accelerating the cyber arms race and elevating each other's capabilities [13]. Early research by Howcroft et al., [14] noted that although consumers' confidence in e-commerce applications was strong, their confidence in technology was weak. In the past decade the Stuxnet attack [15], WannaCry, and NotPetya [16], or American oil pipeline [17] attacks have shown that cyber-attacks are considerably more expensive, disruptive, politically motivated, and strategic. More worryingly an emerging perception by some that taking a more proactive role in cyber-defences are needed.

4. Active Defence

The perception that the driving forces of digital transformation through cyberspace is creating and perpetuating insecurity with potentially catastrophic consequences are evidenced by the recent rise in cyberattacks on critical infrastructure such as oil pipelines in the U.S. and the health services in Ireland [17], [18]. Within this context, cyber security politics may be characterized by the interplay between technology, politics and science. Dunn Cavelty and Wenger [19] noted two main factors; technology use and misuse by human actors and second, conflicting formal and informal negotiation processes between the state and society, the legal boundaries and acceptable rules of behaviour of which are often poorly understood. An emergent perspective that a company may take termed ‘hack-back’ or ‘active defence’ has begun to gain momentum [20]. In this process, a corporate entity may engage in commensurate attacks against the hacker. However, in a paper by Caldwell and Curran [21], they note that as tempting as the hack-back strategy is, there are generally unintended and potentially harmful consequences and warn that hack-back, without due consideration, may only see a compromised server and engage in aggressive tactics to shut the attack down regardless of the server’s main function be it an unwitting and innocent party thus, running the risk of collateral damage being extensive. A more progressive approach in digital transformation that takes security into consideration before such actions is the introduction of security within systems and organisations by design.

5. Security by Design

How can we best ensure that the progress and promise of digital transformation isn’t hindered? Corporate in-house training programmes and web-based training materials alert the end-user to the potential risks associated with computer use in today’s office environment. Mendhurwar and Mishra [2] reported an acceleration in adoption of Internet of Thing (IoT) and social media technologies and as progressive as this might be for businesses creating and delivering value, this also permits the seamless transmission of potentially dangerous malware. With this in mind and given the speed of adoption, the job of the cyber-security professional becomes more complex and time sensitive. Recent research by Dunn Cavelty and Wenger [19] indicated that the influence of artificial intelligence (AI) enabled technology within the context of digital transformation opens new analysis opportunities. Although IoT devices have restricted computing, storage and networking capability which limit the sophistication of cyber-defence mechanisms that can be installed [2]. However, there are many more opportunities for the malicious user to exploit them given their proliferation. AI opens the ability to link elements of cyber security in terms of the speed, scale and complexity. While technologies such as these will be primarily developed by the private sector a potential consequence many be that technology firms will dramatically transform the relationship between public as well as private actors. Security by design leverages the philosophy of security and integrates this early in the life cycle of product development from business case right up to product release. While this is not seen as a panacea for all things cybersecurity related, it has become an important point of departure for many projects within enterprises where reputation and quality of products are vital. To offer a practical exercise that might enhance the understanding of cybersecurity in digital transformation, the red team/blue team exercise developed by the military has shown some promise.

6. From Military to Industry

A security spectrum may be characterized by its opposites, the security professional and the client. Research shows that when the end-users and beneficiaries of a system perceive high controllability of behaviour or feel they are able to perform the policy compliance activities, compliance with the security policy is more likely. Equally, when an end-user has previously experienced a security breach, they are more likely to comply with security recommendations. Cybersecurity professionals restrict communication with contexts that are not secure. From the end-user’s context, utilizing security for computing may be restrictive and frustrating, leading to disinterest in security compliance. By considering the perspectives and contexts of both the security professional and the end-user, a holistic view on the nature of security within an organization may be generated. To practically demonstrate this, Red Team/Blue Team exercises are particularly valuable. In this exercise, a group of security professionals, the red team, attacks, the blue team, defends. These exercises draw their inspiration from similar military exercises which are designed to stress test a combat unit and/or the security of sensitive installations like state run laboratories. The outcome of the exercise results in both parties sharing their results and collaborating on a solution. A practical basis for communication is possible where the language and practices of either party are critiqued in an environment that productively benefits both. This could be a scheduled practice that ensures user confidentiality, integrity and availability of critical assets in the future and help to reduce the chances of intentional/unintentional resource damage, corruption and data breaches. In the longer term, end-users and businesses need to take ownership of their cybersecurity posture by establishing a proper business continuation plan combined with providing training and education about cybersecurity. Within the context of digital transformation, the pervasive need for cyber-physical systems such as our embrace of machine learning with integrated technologies within the Internet of Things (IoT) means that there are several contributions from cybersecurity practices that digital transformation can take advantage of. The outcome of a red/blue team exercise can relate technological developments that are relevant to end-users’ lives and interests at present and may encounter at some point in their lives. This can have a positive effect on end-users' attitudes towards learning more and potentially enhance and improve end-users' perceptions of cybersecurity.

7. Internet of Things (IoT)

Cybersecurity in the Internet of Things (IoT) refers to the practice of protecting internet-connected devices from unauthorized access, malware, and other cyber threats. As the number of IoT devices continues to grow, cybersecurity has become an increasingly important issue for both businesses and individuals. One of the key challenges of IoT cybersecurity is the sheer number of devices that are connected to the internet. Unlike traditional computers, which typically have a dedicated user who can apply security updates and patches, many IoT devices are designed to operate without human intervention. This means that they may be vulnerable to security threats that can spread quickly across a network of connected devices. Another challenge of IoT cybersecurity is the diversity of devices that are connected to the internet. IoT devices can range from simple sensors and smart appliances to complex industrial systems and medical devices. Each of these devices has its own unique security requirements and securing them all can be a daunting task. To address these challenges, businesses and organizations that use IoT devices should implement a comprehensive cybersecurity strategy. This strategy should include measures such as regular software updates and patches, secure network design and implementation, and the use of strong passwords and other authentication measures. Individuals can also take steps to improve the cybersecurity of their IoT devices. For example, they can avoid using default passwords on their devices, and they can use a separate network for their IoT devices to prevent unauthorized access. In addition, they can stay informed about the latest cybersecurity threats and take steps to protect themselves and their devices. Overall, cybersecurity in the IoT is an important and complex issue that requires a multi-faceted approach. By taking steps to secure their devices and networks, businesses and individuals can help protect themselves and their organizations from cyber threats.

The Internet of Things (IoT) and cloud computing are almost synonymous and exemplify the importance of trust. It is the need for interconnectivity that is simultaneously of enormous value in these systems, but also opens vulnerabilities. IoT and cloud computing are dependent on geographically distributed computing entities like storage servers, dedicated systems, and networking software from which private users to corporate servers derive a service. As a result, desktop computers, laptops, mobile phones, tablet computers as well as internet connected devices such as wearable technology now potentially vulnerable access points. Indeed, security in any system is only as strong as its weakest point and unfortunately the IoT this has become much more problematic since smaller devices such as the smart watch, router and mobile phone have a lack of in-built security. The lack of security on IoT devices violate privacy of personal information, show a lack of passwords of sufficient complexity and neglect to implement data encryption. As noted by Medhurwar and Mishra [2], the era of technology convergence necessitates multiple technologies to enable the digital transformation of enterprises in previously unforeseen scenarios.

8. Conclusion

Mary Shelly’s Frankenstein (which has as subtitle, The Modern Prometheus) was written during the first industrial revolution (1817), where society’s relationship with technology wrestled with the consequences of technology and asked the question, are these technological advancements a monster we cannot control? Today, we are wrestling with the same questions two hundred years later except, the problem isn’t one monster, it’s many. In this paper we focused upon broad issues pertaining to complex socio-technical systems which necessitate a commensurate growth in cyber security worldwide. As we struggle to shape our fourth industrial revolution via digital transformation, the changes that may emerge impacting society, economy and the state are in flux. The ubiquitous digitalization and automation of technical processes means that we now regard cyber security at the level of international politics. How new technologies are used in political and business contexts, has brought attention upon theoretical cyber-attack scenarios and moved us towards the reality of advanced persistent threats, necessitating the use of AI given the scale and complexity of attacks within the threat landscape.

9. Acknowledgment

With grateful thanks to Axway.

10. References

[1] Knickrehm, M. B. (2016). Digital Disruption: The Growth Multiplier. Accenture Strategy.

[2] Mendhurwar, S., and Mishra, R. (2019). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems. DOI: 10.1080/17517575.2019.1600041.

[3] World Economic Forum. (2016). What is the fourth industrial revolution? https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/. (Access Da -te: 6 July 2022).

[4] Teo, C., S., and Mahmoud, A., K. (2017). National Cyber Security Strategies for Digital Economy.

[5] Hathaway, M. (2013). Cyber Readiness Index 1.0. http://

www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-1point0.pdf. (Access Date: 2 March 2022).

[6] Chakravorti, B. (2016). Where the Digital Economy is Moving Fastest. Harvard Business Review.

[7] Elkhannoubi, H., and Belaissaoui, M. (2015). Fundamental pillars for an effective cybersecurity strategy. Computer Systems and Applications (AICCSA).

[8] NATO. (2013). NATO, National Cyber Security Strategy Guidelines. CCDCOE. https://ccdcoe.org/uploads /2018/10/NCSS-Guidelines_2013.pdf. (Access Date: 13 April 2022).

[9] UK Government. (2020). National Cyber Security Strategy 2016-2021. UK Cabinet Office. https://assets.publ ishing.service.gov.uk/government/uploads/system/uploads/ attachment_data/file/937702/6.6788_CO_National-C yber-Security-Strategy-20 16-2021_WEB3.pdf. (Access Date: 1 May 2022).

[10] US Government. (2015). The DOD Cyber Strategy. htt ps://archive.defense.gov/home/features/2015/0415_cyber-s trategy/final_2015_dod_cyber_strategy_for_web.pdf. (Acc -ess Date: 4 April 2022).

[11] Suh, B., Han, I., (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. International Journal of Electronic Commerce / Spring. Vol. 7, No. 3, pp. 135–161.

[12] EU Commission (2019). Digital Transformation in Transport, Construction, Energy, Government and Public Administration. ISBN 978-92-76-08613-0.

[13] Moller, D. (2020). Cybersecurity in Digital Transformation Scope and Applications. https://www.sprin ger.com/gp/book/9783030605698. (Access Date: 3 May 2022).

[14] Howcroft, B., Hamilton, R., and Hewer, P. (2002). Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. The Int. J. Bank Mark, 20(3), 111-121.

[15] Baezner, M., and Robin., J. (2017). Hotspot analysis: Stuxnet. Zuich: Center for Security Studies (CSS).

[16] Baezner, M. (2018). Hotspot analysis: Cyber disruption and cybercrime: Democratic people's Republic of Korea. Zurich: Center for Security Studies (CSS).

[17] Turton, W., and Mehrotra, K. (2021). Hackers Breached Colonial Pipeline Using Compromised Password Compromised Password. Bloomberg. https://www.bloom berg.com/news/articles/2021-06-04/hackers-breached-colo nial-pipeline-using-compromised-password. (Access Date: 3 April 2022).

[18] The Journal. (2021). 'Anyone who worked the weekend has aged hugely': Emergency staff under intense pressure amid HSE hack. The Journal. https://www.thejournal.ie/em ergency-department-ransomware-5439513-May2021/. (Ac -cess Date: 14 June 2022).

[19] Dunn Cavelty, M., and Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy. DOI: 10.1080/13523260.2019.1678855.

[20] Messerschmidt, J. (2013). Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm. Columbia Journal of Transnational Law. http://ssrn.com/abstract=230 9518. (Access Date: 9 September 2022).

[21] Caldwell, A., and Curran, K. (2021). A Critique of Active Defense or 'Hack Back'. International Journal for Information Security Research (IJISR). 10(1), 957-961. DOI: 10.20533/ijisr.2042.4639.2020.010.