Convergence and Proliferation of Technologies: Cybersecurity, Privacy, and Risk Management

A.Yarali, R. Joyce, D. Albeloshi, J. Edwards, B. Dixon
Ayarali@murraystate.edu
Murray State University, Murray, KY

Jim Hoag, Ph.D.
jhoag@Champlin.edu
Champlain College, Burlington, Vermont

Abstract - The world nearly completes the transition from being analog to the digital age and digital technology is revolutionizing the way society operates and empowers individuals to participate in social events. The future of business tech will continue to experience exponential growth as more organizations will continue to implement the latest technological advancements to run various functions and processes and businesses are transforming from doing digital to being digital by the wholesale restructuring of their strategic processes Even as the future of business technology continues to get brighter, there is a need to reconsider cybersecurity, privacy, and risk management issues. As technology continues to advance, the risks become more, and thus, security becomes a significant aspect that needs to be addressed. In the last few years, new laws have been developed to regulate how service providers collect, use, retain, disclose, and dispose of user information. The number of cyber-attacks and data breaches have been rising at an alarming rate; it is essential for the organization to take necessary precautions to protect their data. In this paper, transformation and advancement to a pervasive and converged digital infrastructure of AI, IoT, *and big data with their threats and security at all levels of entry points, customer demand, surface attack, and landscape are discussed.*

Keywords

Digital security, Cyber Security, IoT, Cloud, Big Data, Privacy, Risk Management,

1. INTRODUCTION

Cybersecurity, privacy, and risks management is a significant issue that needs to be addressed by organizations. In the next two decades, different trends in technology will impact industry while competitors are expected to implement the latest technological models so that they can increase their market share (Desjardins, 2018). There are various vitals trends and “X-as-a-Service” (XaaS) opportunity proliferation through digital adaption which will disrupt the traditional "brick-and-mortar" industry. Some of these trends include migration of data to the cloud, artificial intelligence where it is expected to benefit businesses and the society at large, extended reality, data veracity, frictionless business, and the Internet of Things (Kambala, 2018) which are crafting a new digital system to cope with increasingly diversified demands, while increasing the endpoints. Businesses today are transforming from doing digital to being digital by the wholesale restructuring of their strategic processes to cope with technical, innovation, customer and market agility.

The goal of most of the technological advancement is to improve on exciting infrastructures, increase efficiency, speed, security, and quality. With the rise in technological advancements and diversification, it is essential for organizations to consider strategic partnerships or acquisitions as they seek to increase their market share. Partnerships and acquisitions are meant to provide organizations with a competitive edge. Corporate partnerships give organizations a competitive edge by acting as an alliance that allows them to promote each other's services and products. In the next two decades, more acquisitions and partnerships will occur as organizations will be seeking to enhance their modes of operation (Maras, 2015). In industries like manufacturing, agriculture, biomedical and energy digital transformation and convergence occurring at all physical levels. As technology continues to evolve, there are both best practices and complex and changing set of risks that are associated with it. In this case, the best practices of the emerging technology involve efficiency whereby since time do not stand still, there is a need to have things done quickly and accurately (UN, 2018).

In the healthcare sector, the business has changed tremendously since the presence of different technological machinery has enhanced the diagnosis of different diseases and infections, and thus, it is easier to get cured. The inventions of different technologies are changing business dynamics constantly shifting from enterprise driven trend to consumer-driven market. Another best practice that has been established by the presence of technological advancement is safety. In this case, industries and manufacturing sites are safer, and thus, hazards that could affect peoples' health have been minimizing (UN, 2018).

Even though there are numerous advantages associated with emerging technologies, they are posing some risks in various areas which requires security mandate and continues assessment of their cyber risk profile and proactively manage their defense (Aon, 2019). Once an idea has been published on the internet, either positive or negative, it is difficult to remove it and can easily be traced back to the owner. As a result, it is possible for some individuals to post misleading information that could impact businesses negatively (Ramey, 2012). The presence of global networks has enabled malicious actors with motives to spearhead negative propaganda towards their competitors, and this could hurt businesses. In the recent past, identity theft continues to be a critical threat for organizations and individuals because of the impact it can have on their virtual image (Veletsianos, 2018). Therefore, even though the emerging technology has benefitted individuals and organizations at large, the negative issues need to be addressed so that the goals of technology advancements can be achieved successfully. For example, an autonomous car already includes cellular, Wi-Fi, Bluetooth, Infrared and other technologies to come which this translate into growing cyber attack

2. EVOLVING LARGE-SCALE TECHNOLOGIES

Big data and data analytics are expected to change insights about the customers, operational costs, and all the relevant aspects of different business models around the world. The emergence of cloud computing has enabled businesses to compete at a higher level since the traditional software and systems are no longer required. Digital heterogeneity and the confluence of Artificial Intelligence with 5G and IoT are expected to dominate the market since the majority of the organizations in the world are considering the use of AI to reduce their operating costs. In two decades, the number of AI-fueled organizations will increase as they seek to enhance their performance and to provide high-quality products and services (Tredinnick, 2017). Another aspect that is expected to redefine the connectivity of tomorrow is the rising number of connected devices. The number of network-connected devices is multiplying, and this has led to a positive impact on both the wireless and wired technology ecosystem. Therefore, the connectivity of tomorrow will enhance different services where the organization will choose the ideal mode of services to meet customer needs. As business tech continues to grow, the number of products, services, and business models is expected to rise. Innovations within organizations are expected to rise to meet the ever-increasing demands of the customers (Herbane, 2010). Organizations can drive the technology strategy through their investments to ensure they meet the demands and requirements from their customers.

2.1 Cloud Computing Environment

Growth in cloud computing has helped companies to minimize their cost since the solution is better as compared to traditional modes of operations. The presence of cloud computing has also promoted advancement in intelligent interfaces that promise a better future for the business. There is not a single and clear-cut definition of cloud computing, but suffice it says that off-site services provided to allow for a reduced on-site required hardware and software and subject matter experts are the overarching goal of cloud-based services. A downside of

Cloud environments is that they rely significantly on third parties to make decisions about their data, and when this comes into play, it makes security even harder to implement. The continuous transition from vertical and corporate data centers to a shared platform of the cloud is changing the cyber risk. Multi-tenancy is a distinctive feature of public clouds. Some of the unique security and privacy implications in cloud computing are (Hassan Takabi) :

a. Outsourcing Data and Applications - One of the biggest, and most recurring themes of this are that customer data is stored off-site and therefore susceptible to different, potentially less stringent, forms of security.

b. Extensibility and Shared Responsibility - Depending on the type of cloud services procured, the levels of security range from fully implemented upon purchase, to entirely dependent on the customer to implement hardening techniques and access controls.

c. Service-Level Agreements - SLAs are the agreement between the cloud provider and the customer who is utilizing the cloud environment. The SLA outlines basic requirements/needs and identifies what level of service is expected. Service level agreement is the contract that stipulates what levels of support/security the customer expects and is paying for.

d. Virtualization and Hypervisors - The ability to have a single system operating multiple OSs at the same time is critical to cloud computing. Being able to split hardware resources between multiple clients provides the ability to fully utilize the hardware most productively, but also requires management tools that ensure cross-pollination between the multiple instances does not affect each other.

e. Heterogeneity - It is already implied, but just to further the point, when using cloud services there is an innumerable amount of differences between the needs and usages of customers. Hardly any two customers are going to want the same thing, so the ability to have systems operating in different capacities/levels is a must.

f. Compliance and Regulations – With the ability of outsourcing data management, comes the question of how it is regulated. This poses many concerns because the data may be housed/managed in a location with different requirements than where it originates such close coordination between the customer for their requirements and the provider with their capabilities is a necessity

When storing data in the "cloud," customers need to be aware of the security concerns that accompany off-site storage of data, such as multi-tenant domains, shared resources, access control policies and implementation of approaches designed to prevent/restrict unauthorized access to private data. There are several mitigating techniques available, but not a lot of accepted standard practices. They offer up several possibilities/recommendations, but at the end of the day, it is just one group's opinions on the best approach to answer these questions. The current best approach for securing cloud bases services is to conduct a security audit and risk assessment. Performing both these provides the customer and provider a clear understanding of what risk exists by using their system, what level of security is expected/defined in the SLA, and any residual risk that remains and how possible it is to further mitigate the residual risk with customer (in-house) policies and practices. Some cloud providers will very obviously be ill-equipped to provide the level of security necessary, while others will cost too much to use. Somewhere in the middle, most customers will find a cloud provider that provides adequate data protection at a reasonable cost, but what is reasonable is subject to each company's data storage requirements. Some of the security and privacy approaches are as follows (Hassan Takabi):

a. Authentication and Identity Management – Authentication is a crucial component when granting access to data, and cloud-stored data is no different. Before allowing access to data, the cloud service needs to confirm that the person requesting access is approved to access the data requested.

b. Access Control and Accounting – It should go without saying, but it doesn't, if you need to authenticate someone, you also need a traditional method/technique for determining what access they receive one authenticated and way to maintain records of the event.

c. Trust Management and Policy Integration – Assuming authentication is determined, cloud computing requires additional controls to ensure access is not granted to adjacent cloud systems. This goes hand-in-hand with the AAA techniques discussed above.

d. Secure-Service Management – This section does not say anything new when procuring/using a cloud-based system, the customer needs to ensure the security provided meets the level of security desired, and there is a mechanism/outline in place to ensure continued data privacy.

e. Privacy and Data Protection – Yep, as already discussed, cloud bases services must have in place a technique/service/control to disallow unauthorized access to data stored remotely. Storing data in the cloud inherently means that the data is more susceptible to breaches, so a thorough review of the provider and their security policies is needed before contracting their services.

f. Organizational Security Management – A couple of additional concerns are introduced, such as: when sharing cloud space with someone who is a more prone target than yourself, are you accepting/inviting more risk toward your data. Also, concerns over natural disasters should be considered, but not for the customer, more appropriately for the cloud service provider.

2.2 Artificial Intelligence

The emergence of AI has promised to change the world, and in the last few years, it has impacted people's lives positively. Different businesses are currently capitalizing on the potentials of AI; hence they acknowledge that it will revolutionize different businesses in the next two decades. AI is more than a tool, and it has changed the functionalities of different businesses (Kambala, 2018). AI will continue to revolutionize digital marketing, and ads, based on the core values of a business or an organization. The presence of extended reality aimed at ending the distance by connections between people has transformed the way people work and live. In the next few years, this form of technology is expected to limit the distance between people, information, and experiences via digital connectivity empowered by the internet and mobile. As a result, the business will benefit from these changes since employees can work from any location resulting in higher productivity and turnover (Manyika et al., 2013). Although the digital data often contains biases, noise, and abnormality in two decades the data veracity will transform and help to filter for more in-depth understanding of how to deal with different vulnerabilities.

Data veracity is the degree to which data is accurate, precise and trusted. Moreover, is an emerging trend that is meant to determine if business insights may be corrupted and help the management to avoid skewed decisions. It is essential for the organizations to address the issues associated with data bias, inaccurate and manipulated data trends and ensure they run the organization effectively (Manyika et al., 2013). It is vital for organizations to redesign themselves as they get ready to embrace frictionless businesses where they can build to partner at scale. One of the emerging trends is that businesses are depending on technology-based partnership as they seek to grow. The partnerships are meant to expand the partner networks faster than it was the case before (Manyika et al., 2013). The establishment of robust digital ecosystems will enhance business relationships between the organizations, and this will guarantee a brighter future.

2.3 Internet of Things

Internet of Things (IoT) is another emerging technology that will continue to revolutionize business in the next two decades (Kambala, 2018). It involves the interconnection of different devices over the internet where it allows people to communicate, and run different applications. IoT allows people to control their home heating, lighting, sprinklers, and many other appliances through their mobile devices (Manyika et al., 2013). These solutions have revolutionized business, and it is a trend that is expected to grow tremendously in the next few decades. It is expected that the integration of IoT will affect and disrupt many businesses since it provides unprecedented opportunities through process automation and data gathering processes.

The Intent of things is everywhere, and it is creating more risks than firms realize. Integration of vulnerable massive IoT devices to cellular and high-speed 5G technology creates new paths of cyber-attack. While this massive connectivity enhances operational efficiency and quality, it also creates a situation where the attacker can move across the network by penetrating through the equipment designed with no security. An expanded network of IoT connectivity such as smart city has a high potential that the security risk may cascade through the whole city infrastructure. Having a well-defined architecture for IoT is essential to maintaining the integrity, confidentiality, and availability of the information and IoT devices. Constant inventory and monitoring IoT devices by an organization is necessary to evaluate the risk associated with these endpoints. In the perception layer, there are four main security mechanisms of authentication, data privacy, the privacy of information, and risk assessment. The perception layer handles the authentication mechanism by using cryptographic hash algorithms that provide the digital signatures to the clients. Symmetric and Asymmetric encryption is used to accomplish data privacy for IoT devices at the hardware level since IoT devices are often low power consumption with a small footprint and or low computing complexity [Farooq, 2015]. To ensure that sensitive information remains private on the IoT devices the K-Anonymity approach is used to protect this information [Emmam, 2008]. For the risk assessment mechanism, the regular assessments of the IoT devices will help to find new threats to the system(Yarali,2019).

IoT technology has grown exponentially in such a short amount of time and with this growth, new challenges have arisen that still need to be overcome. The growing popularity has made IoT a standard in future technology for the Internet, communications, and physical world monitoring. The architecture of the IoT has yet to be standardized and needs to be protected at every layer. In developing these standards, security is essential to the process so that every component in IoT is protected. The challenges and room for potential methods of security for IoT will continually need evaluation as this technology progresses

3. DIGITAL SECURITY

Cybersecurity, privacy, and risks management is a significant issue that needs to be addressed by organizations. Despite the rising growth in technology, data security is a critical aspect that should be addressed (O'brian, 2012) at entry points, customer demand, landscape and attack surface. Threats and attacks are external or internal targeting at the front, back and next door, accountability, and transparency of customer, complexity and increased connectivity (Hawng, 2019). There is a need to enhance cybersecurity protocol, implement privacy models and implement the ideal risk management processes that can be used during threats. Therefore, the future of business tech is bright, and thus, organizations should be ready to experience disruptions and changes as they embrace the ever-changing trends in the industry.

Even as the future of business technology continues to get brighter, there is a need to reconsider cybersecurity, privacy, and risk management issues. As technology continues to advance, the risks become more, and thus, security becomes a significant aspect that needs to be addressed (Cleary & Felici, 2014). In the last few years, new laws have been developed to regulate how service providers collect, use, retain, disclose, and dispose of user information. The number of cyber-attacks and data breaches have been rising at an alarming rate; it is essential for the organization to take necessary precautions to protect their data. The future of business technology is expected to experience data privacy and regulatory space (Herbane, 2010). In 2018, the EU regulatory space started sweeping changes regarding privacy and data security policies where all the organizations were meant to implement the laws that govern how they manage and share user’s data. Cybersecurity, privacy, and risk management are essential in any organizations; the stakes are higher than ever since the risks will continue to grow. They will continue to face risks associated to privacy and security practices, and thus, it is essential for the organizations to implement the ideal policies that will enhance security and protect user data (Maras, 2015).

Cybersecurity involves protecting and recovering networks, network devices, and various programs from any form of cyber-attack. In the current IT world, cyber-attacks are common, and if networks are not well protected, the attacks could result in the destruction of sensitive data and money extortion. Privacy aims to secure user information and protect it from getting into wrong hands. Personal information is confidential and thus, it is one of the distinct components of information security. Therefore, it is essential to enhance privacy to ensure that user data is protected and cannot be accessed by unauthorized users (Rademaker, 2016).

Risk management involves identification, analysis, and assessment of various risk in cyberspace. It involves studying and analyzing the information technology infrastructures and identifying all the possible vulnerabilities that could impact different systems negatively (Maras, 2015). Once the assessment has been done, the ideal risk management is to be done where program priorities are identified various process are initiated to monitor, control, and minimize the risks. Under cyber Security, privacy, and risk management, the internal and external risks are established where the ideal framework of risks management is identified. It is essential to define the communication lines involving all the stakeholders so that the consequences of the risks can be highlighted and the status of the risks can be analyzed for a solution to be formulated (O'brian, 2012). It is a process that needs prioritization to reduce the chances of risk occurrence while at the same time establishing processes that will enhance risk review processes.

4. EDUCATION

How do we ensure the next generation of Cybersecurity Professionals? Topics such as IoT, Big Data, and AI need to be integrated into Cybersecurity education. While some programs cover the risk, cloud computing, and IoT the comprehensive impact and issues on designing securing systems and analyzing incidents will require additional and broader perspective. While there are courses at many schools in these areas, that content may be siloed. Efforts need to be made to make cybersecurity curriculum interdisciplinary because of the benefits of efficiently using institutional resources (Chen, & Cotoranu, 2013). The National Initiative for Cybersecurity Education (NICE) framework that the National Institute for Standards and Technology (NIST) outlines introduce cybersecurity skills and knowledge units for curriculum that needs to be taught in an institution. The framework categorize areas into specializations that could be expanded to encompass the areas of AI and Big Data and coin it as cybersecurity analytics. While the Colloquium for Information Systems Security Education (CISSE) advocates for cybersecurity education at all levels and could help advocate for these areas to be integrated into cybersecurity curriculum. Another route that the cybersecurity analytics could be added into cybersecurity curriculum is through the Centers of Academic Excellence in Cyber Defense (CAE-CD). Institutions that have this accreditation that has proven they teach specified knowledge units in the realm of cybersecurity and the accreditation process allows institutions to have specializations like Healthcare Security. Specialization could be created to encompass the areas of AI and Big Data. With these possible avenues for expanding the cybersecurity curriculum, there are many opportunities to keep the curriculum on the bleeding edge of cybersecurity technology and practices.

5. CONCLUSION

In the next two decades, it is expected that more regulations will be developed as organizations will continue to adopt technological advancements to enhance their performance. As more organizations implement digital technology, the risks associated with it will continue to rise. Therefore, it is the mandate of the management team to enhance privacy, implement the ideal cybersecurity techniques, and establish a risk management process that will help them to deal with cyberspace threats. Some of the risks that may expose an organization to hackers or intruders include the presence of limited configuration security, lack of patch management, lack of proper encryption process, and weaknesses in code security. These weaknesses expose systems and could harm the organization's data. Therefore, it is essential to implement cybersecurity techniques, privacy and risks management process that will ensure the organization is protected at any given time. Some of the ideal mechanisms that could be used to strengthen cybersecurity include enhancement of network security, OS and database security, front end security, authorizations for users, communication security, and the presence of emergency concepts where backup and disaster recovery processes are defined. The explosion in internet penetration is a tremendous boost to organizations around the globe, but Cybersecurity is the primary concern that needs to be addressed since the same organizations are exposed to significant threats. The future of business technology is bright, but it is essential for organizations to consider the ideal practices that will keep them off from cyber threats, risks, and privacy issues.

6. REFERENCES

[1] AoN, 2019 Cyber Security Risk Report: What is Now and What is Next. February 2019.

[2] Cleary, F., & Felici, M. (2014). *Cyber Security and Privacy*. Cham: Springer International Publishing.

[3] Chen, L. C., & Cotoranu, A. (2013). Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices.

[4] Emam, K.E., F.K. Dankar, Protecting Privacy Using k-Anonymity, in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[5] Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis of the security concerns of the internet of things (IoT). International Journal of Computer Applications, 111(7).

[6] Herbane, B. (2010). Risk Management on the Internet. *Risk Management*, *7*(1), 71-72. doi: 10.1057/palgrave.rm.8240206

[7] Hassan Takabi and James B.D. Joshi *University of Pittsburgh &* Gail-Joon Ahn *Arizona State University.* Security and Privacy Challenges in Cloud Computing Environments Computing Now, IEEE Computer Society, Novwmbwer-December 2010.

[8] Hwang, Dew (2019). Digital Transformation (DX). WTS2019, NY, April 9-12.

[9] Kambala, C. (2018). What the Internet of Things Means for Businesses - DZone IoT. Retrieved from https://dzone.com/articles/what-the-internet-of-things-means-for-businesses

[10] Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). Disruptive technologies: Advances that will transform life, business, and the global economy. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Executive_summary_May2013.ashx

[11] Maras, M. (2015). Internet of Things: security and privacy implications. *International Data Privacy Law*, *5*(2), 99-104. doi: 10.1093/idpl/ipv004

[12] O'brian. (2012). *Cloud computing strategy*. [Washington, D.C.]: Chief Information Officer, Dept. of Defense.

[13] Rademaker, M. (2016). Assessing Cyber Security 2015. *Information & Security: An International Journal*, *34*, 93-104. doi: 10.11610/isij.3407

[14] Tredinnick, L. (2017). Artificial intelligence and professional roles. *Business Information Review*, *34*(1), 37-41. doi: 10.1177/0266382117692621

[15] Yarali, A., Srinath, M., Joyce, R., (2019). A Study of Various Network Security Challenges in the Internet of Things. WTS2019, April 9-12, 2019, NY.