Telecom Business Review
13 (1) 2020, 65-68
http://publishingindia.com/tbr/

Building the Next-Gen Cyber Security Operating Model in a Digital Eco-System

Niladri Shekhar Dutta

Director, TMT and Digital. Email: niladrishekhar.dutta@gmail.com

Abstract

The business of today are fast changing from a pipeline based model to a platform based model. The Digital businesses of today are focussed on this simple strategy which makes them use and rely more on technology enablers. These companies create new value and experiences that differentiate them with a competitive edge over their peers. New value is created in business models, customer experiences and the internal capabilities that support core operations of an organization. Thereby in the tech space, organizations transforming the programs to become digital business enablers, is very crucial in order to create an exponential value in this era.

A core entity due to this rapid transformation is Cyber Security and the blueprint which one needs to adapt within this ecosystem of devices, applications and interfaces. Due to requirement of enabling digital business, during digital transformation and afterwards organizations are exposed to different risk factors and situations which cannot be handled and detected by utilizing the conventional and existing security practices for IT. This paper essentially focusses on stitching the various capabilities that entails the need and desire of a winning proposition which stands in front of CxOs to start thinking of Risk management and Cyber Security in a very different light and how one can leverage this function to show its direct and indirect benefits. It must address a new reality in which IT organizations have little direct infrastructure, and their biggest security concerns will come from services outside their control eg. using cloud services. That is why it is required to build a Security operational model architecture in the Digital Business World. A Security operational model will integrate all required crucial capabilities along with the security operational processes, skills, infrastructure, security enablers and drivers of customer/ user experience followed by the next gen DNA which need to exist within the whole organization set up. This will eventually ensure better performance and even overcoming pitfalls of the processes by complementing each other and also adding value in terms of providing better customer experience, optimizing cost price, reducing time of operation and other conveniences compared to earlier individually existing conventional security methodologies. In order to create an effective and secured blueprint which will provide fruitful results due to transformation to digital business approach should be initiated by considering having a proper vision as the first and initial step, followed by changes in objectives, embracing principles to ensure trust resilience and developing an adaptive, Context Aware Security Architecture. Ensuring security is very crucial in different real world scenarios such as remote management of IT resources, shared cloud services, encrypting data in motion and rest, effective management of BYOD devices etc.

Keywords: Cybersecurity, Digital Business, Digital Transformation, Risk Management

1. Introduction

The changing competitive landscape has pushed a lot of industries and domains towards adoption of technologies and operating models, leading to creation of a new digital eco-system. This adoption is driven by consolidation and collaboration in the market, a need to identify new revenue streams to maintain the profitability, ways to enhance the customer experience and to remain higher in the evolving and merging value chain. As the boundaries blur and businesses move towards platform based model/new digital business models, the complexity in the eco-system increases with multiple partnerships and joint ventures.

1.1. Objective

No sector or industry whether it's Retail, IT, Communication, Media & Technology or Finance, has been left untouched by the atrocious hackers and security attackers. They have marked the headlines, incurring major data and security breaches costing them not only their revenues but also compromising their brand value. The ubiquitous nature of vulnerability can be explained due to the dissolving perimeters caused by more connected environments than before, adoption of new technologies like – Cloud, APIs, IoT devices, Mobile payments, M2M, BYOD etc (Choi, Kaplan, Chandru & Harrison, 2019). (Douglas & Loader,

2000) These technologies though enabling faster digital adoption are also increasing the touch points/threats for data and cyber security breaches. These security threats which were earlier handled reactively need to be catered more proactively in today's interconnected and complex eco-system.

2. A Sneak Peek into Past

Cybercrime can be considered as illegal activity which is done over networks connected over internet. It is perceived as unauthorized entry into network system with a motive to delete, modify or steal organizational data.

In some cases the motto of cyber criminals is to hack the digital ecosystem and steal the money from it. In other cases, the intention of cybercriminals is to cause reputational risk and therefore, they block the servers such that nothing can be accessed from it.

Cybercrimes are commonly considered for two types of crimes: new offences committed using new technologies such as offences against data and computer system, dealt with in the Computer Misuse Act 1990 and old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence.

Lastly there are huge number of researches done in past on cybercrimes and security laws and conventional way of mitigating issues. Very less research is done on use of technological models in digital ecosystems to prepare such security models that will understand, mitigate and develop auto solutions in order to prevent such attacks on an organization security in future. Hence this research is based of analysing and building operational security models using cutting edge technology.

3. The Changing Landscape of Cyber Security

Cyber Security is no longer the responsibility of just IT function but should run down from the CEO of the organisation to the lowest rank employee. It has emerged as a board room discussion and is more often than not considered as an enabler of risk transformation to drive efficiency, effectiveness and indirect cost benefits. The organizations of today are focused on building cyber war-gaming capabilities with real life simulations with component based operating model dimensions which would help look some of these ideas pragmatic and operational.

The stakes though are higher because of the magnitude of the advanced persistent threats and sophisticated malwares; it also presents an opportunity to look the security domain under a different light. The providers as well as consumers are moving towards better understanding on the importance of a robust cyber security operating model and strategies.

A core entity due to this rapid transformation is cyber security and the blueprint which one needs to adapt within this ecosystem of devices, applications and interfaces. Due to requirement of enabling digital business, during digital transformation and afterwards organizations are exposed to different risk factors and situations which cannot be handled and detected by utilizing the conventional and existing security practices for IT. This paper essentially focusses on stitching the various capabilities that entails the need and desire of a winning proposition which stands in front of CxOs to start thinking of Risk management and Cyber Security in a very different light and how one can leverage this function to show its direct and indirect benefits. It must address a new reality in which IT organizations have little direct infrastructure, and their biggest security concerns will come from services outside their control eg.using cloud services. That is why it is required to build a Security operational model architecture in the Digital Business World.

An effective security strategy should be the one which cuts across all the levels of the organisation and also takes into account the partners and end customers. Hence, the need of a new cyber security operating model which serves the digital eco-system. The cyber security model should be first of all in alignment with the Business Vision. It cannot work in solidarity from the business's core strategy as it used to be before. Since all the threats don't pose as much damage, focus should be on identifying major threats and the domains affected by them. The principle should be to Detect, Assess, Prevent and Respond. With the advent of strict GDPR regulations and other evolving regulations in the security world, regulatory compliance should form a prominent building block for the model.

4. Solution

Currently as stated cyber security models have a much decentralised approach in most of the organizations. They cater to threats as and when they come, mostly handling different malwares or threats through a plethora of different products. But considering the digital eco system, the need is to have a centralized cyber security model which can

uniformly prevent advanced threats on a business's entire infrastructure. It should not only respond holistically to the current attacks but also leverage emerging technologies to be prepared for any kind of advanced threats or malwares.

The initial foundation for the next generation cyber security operating model should be based on having a Business Vision for Security and Risk management functions which is in alignment with the Organization's core Values and principles. The strategy should be based not only on the current capabilities but also what the organization aims to achieve in the upcoming future. The current risk and security capabilities should be assessed leading to identification of the changes required to create the new competitive capabilities. Once it is identified the security goals should be defined in alignment with strategic management of security risk. Focussing on a risk based approach for security initiative will help in a more balanced and proactive response towards the current generation of security threats.

A Security operational model will integrate all required crucial capabilities along with the security operational processes, skills, infrastructure, security enablers and drivers of customer/user experience followed by the next gen DNA which need to exist within the whole organization set up. This will eventually ensure better performance and even overcoming pitfalls of the processes by complementing each other and also adding value in terms of providing better customer experience, optimizing cost price, reducing time of operation and other conveniences compared to earlier individually existing conventional security methodologies. In order to create an effective and secured blueprint which will provide fruitful results due to transformation to digital business approach should be initiated by considering having a proper vision as the first and initial step, followed by changes in objectives, embracing principles to ensure trust resilience and developing an adaptive, Context Aware Security Architecture.

Once the capabilities and goals are identified, the need is to ensure that there are in-place KPI/KRI metrics to measure the approach. This will help in rationalising the required digital capabilities to meet the risk management and security goals. An organization faces a lot of risks and threats, a targeted approach will lead to a more balanced utilisation of resources for increasing the security resilience. Once identified these targeted capabilities need to be mapped down to the core digital pillars of any organization i.e. Process, System, Organization and People. Security architectures should be designed in such a way that it manages the current as well as future generation of security attacks. Flexible and integrated products/platforms should be leveraged through alliances to have a centralised response to the attacks. Business processes should be articulated in alignment to the security and risk management goals.

The entire well placed cyber security model cannot function effectively unless and until every employee of the organization is made aware of their role in the security and risk strata. A Governance model will ensure that the security and risk management capabilities are distributed and embedded in the organization's culture and DNA. Proper awareness and trainings will help all the stakeholders understand their respective responsibilities for which they can be held accountable for. Partners and other external stake holders should also be made aware about their contribution in this secured eco-system. Proper role assignments will ensure better calibration of the changing regulations and standards. Thus, aligning cyber security and business with each other, will create a symbiotic relation that benefits both.

5. Conclusion

Security or Cyber in general in the context of Digital can no longer be looked upon as siloes entity. One needs to be look at the larger big picture of Digital and then try and amalgamate an integrated Blueprint which would act as an operational best practice pre-cursive model enabling Digital transformation initiatives of which Cyber Security is just one of them. To be in pro-active mode and understand the pre-emptive measures defined by the capabilities of the Security Operating Model should be an integral part of adoption of best practices. Cyber-attacks and threats have exposed the security and risk vulnerabilities of almost all the industries, costing them money and trust of their customers. Thus building the components of the Security Operating Model is not just a best practice but a proven necessity in the modern context of Digital. The advanced nature of threats and data breaches urge for a more proactive security response from the organizations. A well-crafted cyber security model stitched closely in accordance to the digital ecosystem will enable the organizations to achieve their business goals faster and in a more secured manner than ever.

References

Alstyne, M. W., Parker, G., & Choudary, S. (2016, April 06). Pipelines, platforms, and the new rules of strategy. Retrieved from https://hbr.org/2016/04/pipelines-platforms-and-the-new-rules-of-strategy

Choi, J., Kaplan, J., Chandru, K., & Harrison, L. (2019). *Perspetives on transforming cybersecurity.* USA: Digital McKinsey and Global Risk Practice.

Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). Security of today's online electronic. In J. Claessens, V. Dem, D. De Cock, & B. Preneel, *Computers & Security* (vol. 21, no. 3, pp. 253-265). India: Copyright © 2008 Elsevier Ltd.

Deloitte. (2014, September 22). CIO insights and analysis from Deloitte. Retrieved from https://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/

Lainhart, J. W., Fu, Z., & Ballister, C. M. (2016). Holistic IT governance, risk management, security and privacy: Needed for effective implementation and continuous improvement. *ISACA Journal, 5.*

Kannan, S. (2017). Disruptions in retail through - Reimagining the store of the future. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/CIP/in-cip-disruptions-in-retail-noexp.pdf

Sarrab, M., Aldabbas, H., & Elbasir, M. (2013). *Challenges of computer crime investigation in North Africa's countries.* The 14th International Arab Conference on Information Technology (ACIT'2013).

Siddique, M., & Rehman, S. (2011). *Impacts of electronic crime in Indian banking sector.* India: ACADEMIA.