The Cybersecurity Challenge in the Age of Digital Transformation

– Samir Pawaskar

It would be very uncommon if in today's age you have not come across terminologies such as Digital Transformation, Industrial Revolution 4.0, Smart whatever…and this is not just restricted to businesses, we have been so subsumed by such technologies that we now talk of Digital Governments, Smart Nations and this is not just jargon or thin air….

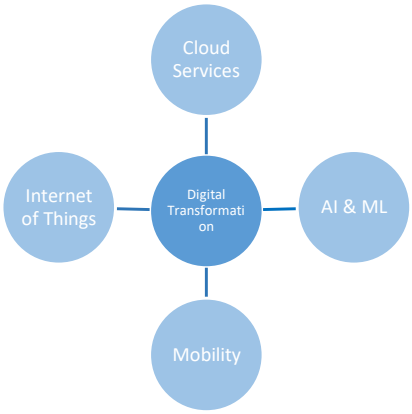
Stuff that we watched in Hollywood movies as kids is a reality today. There is not a single aspect of life that has not been touched and transformed by this technologies. These technologies have now pervaded Agriculture, Health, Manufacturing, Defense, Transportation, Education, Service Industries and what not…

So well it looks and probably it is very cool, with all these gadgets and technologies being able to do stuff that probably a few years back was presumed impossible!

So what exactly is Digital Transformation? Putting it simply, Digital Transformation is the use of technology and data to drive innovation and better business outcomes. Primarily it endeavors to achieve key business goals such as operations optimization, customer engagement and enhanced experience, increased market shares, business agility and better performance.

To achieve this goals Digital Transformation primarily relies on the following technologies:

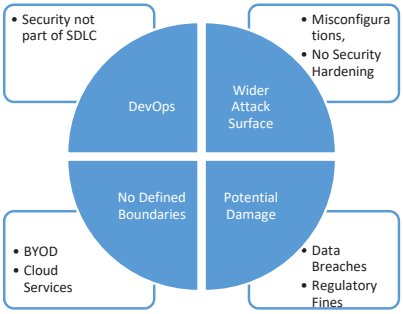
- ✓ Cloud Services
- ✓ Internet of Things
- ✓ Mobility
- ✓ Artificial Intelligence and Machine Learning



So what is the concern here? What am I worried about or rather what should we all be worried about?

Technology is the proverbial "Double Edged Sword", as much as ease and comfort that it drives in to our lives, the technology and the information that is generated, processed or goes around this technology, if not controlled adequately has the power to disrupt our privacy, in the hands of our enemies can be used to launch attacks against us (not necessarily life threatening but that is a possibility as well…)

The use of technology and the immense information introduces the following threats for our businesses:



- ✓ A Wider Attack Surface
- ✓ Increased Potential of Damage
- ✓ Networks without defined boundaries
- ✓ Constant Changes (DevOps)

A Wider Attack Surface:

As more and more processes become digitized, the number of applications, systems and data grows, increasing the opportunities for a malicious actor to compromise them. Further as more and more systems become inter-connected, a potential breach in one

part could allow easy lateral movement for the malicious actor throughout the network and systems.

Increased Potential of Damage:

The potential for damage is huge, as systems are being digitized end-to-end up to the last mile. The trend has moved into critical infrastructures as well. Manufacturing plants, Oil fields, Energy Generation and Distribution, Agriculture, Health Services etc., are all being digitized. A breach in the systems could be far reaching and impact hundreds and thousands of people and could even be life threatening…

Further as "Information" gains value, malicious actors have been known to breach and exfiltrate data. Besides the direct cost (loss of proprietary or commercial information, loss of reputation and customer confidence etc.) due to loss of such information, organizations may have to spend millions by way of regulatory fines, law suits and breach notifications.

Network without defined boundaries:

The concept of a network (enterprise) perimeter that most of the IT Network and Security engineers (Currently in their 30s and 40s) grew up with does not exist anymore. If there is one place on this earth where we have been able to do away with boundaries it is probably the current IT infrastructure.

This in turn does away with ownership and accountabilities, which in turn springs questions on policies and enforcement. How do organizations enforce security policies on systems that they do not own in entirety or are shared across globally?

This requires a paradigm shift in our understanding, our expectations, innovative controls and security strategy.

Constant Changes (DevOps)

The rush to reduce the "Go to Market" has ensured that Software Development teams have quickly adopted methodologies such as DevOps, Agile, and Kanban etc. These ensures that developers can now quickly create and update software. However, the speed of change makes it more prone for security vulnerabilities to creep in especially if security processes are not adhered or integrated within such methodologies.

All this coupled with a lack of visibility resulting from a legacy of non-integrated, siloed, multi-vendor point defense products creates enterprise blind points for the security teams, decrementing their ability to identify anomalous behavior and rapidly mitigate threats.

So how can the businesses deliver security assurance while embracing Digital Transformation?

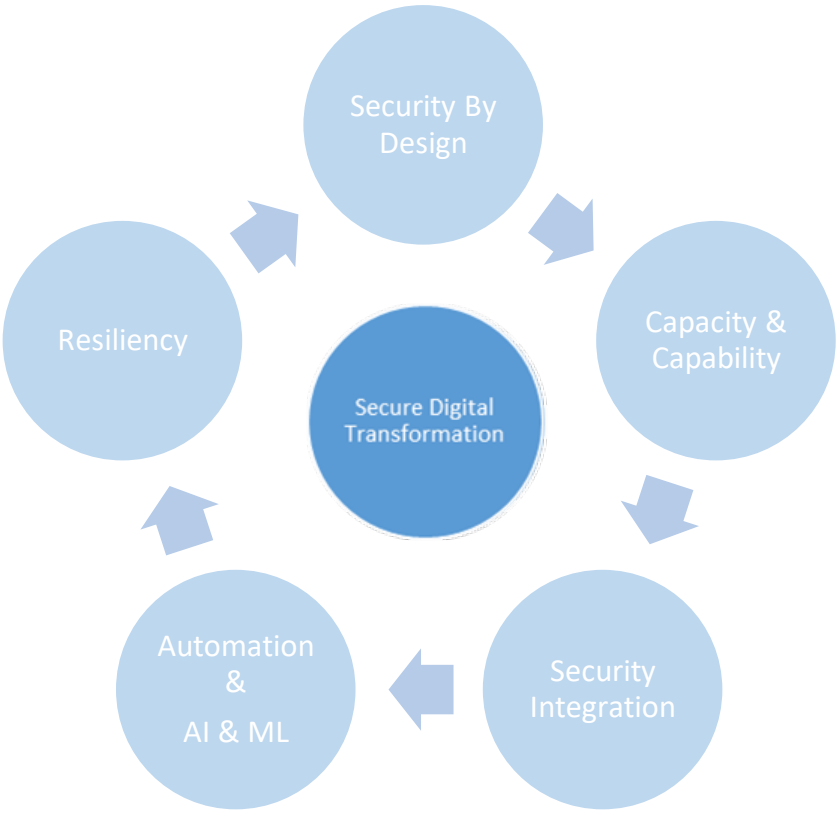
The most important thing that businesses should understand that Security is a MUST, it is not a choice and neither is it a luxury. Having said that, it is important that Security becomes an integral part of the Digital Transformation program, in more than one ways, Security itself should undergo this Digital Transformation to be able to mitigate the risks emanating from such a program. Following are some of the best security practices that will help businesses in their Digital Transformation journey.

Security by Design: Ensure that applications and devices have built in security controls. Use secure software development methodologies. Ensure that default security controls and settings are enabled. Adhere to internationally accepted best practices and security standards.

Build Capacity and Capability: Security is not a "One Man Army" job. Businesses will need to have a proper team with adequate skill sets to be able to secure and defend your business against cyber adversaries. The employees need to be trained from time to time to ensure currency of skills. Using specialized outsourced services could be another option.

Security Integration: It is important to avoid Security Blind Spots and improve security visibility within your organization. This involves ensuring that all the relevant teams, processes and the technology used to secure your organization is integrated and talking to each other. Threat Intelligence should be shared amongst all teams including IT teams. Further, as more and more physical security controls become automated (CCTV, Access Control for Doors, Intruder Alert systems etc.) the interplay between them increases driving the need for businesses to also look at options of integrating or increasing interaction between the IT and Physical security teams.

Transform Security- Use Automation, AI and ML: Automation of security processes can help businesses continuously monitor growing number of sophisticated cyber security threats and expand cyber protections, even with limited personnel and resources. Systems based on Artificial Intelligence coupled with Machine Learning can help businesses detect attack patterns in a fully or semi-automated fashion. They can also



identify indicators of complex attacks, which are hardly identifiable to human centric monitoring.

Build Resiliency: Perform regular testing of systems to uncover potential vulnerabilities and opportunities to improve security. These include Vulnerability Assessments, Penetration testing and of late corporate Bug Bounty programs as well. Businesses need to build practical and effective Disaster Recovery and Business Continuity Plans. Such plans should be exercised at regular intervals. Businesses should also simulate end to end business disruptions through custom built scenarios executed in a Cyber Drill. Se

Disclaimer: This disclaimer informs readers that the views, thoughts, and opinions expressed in the text belong solely to the author, and not to the author's employer, organization or other group or individual.

Samir is an experienced information security professional with more than twenty two years of experience having worked in diverse verticals such as Telecommunications, Government, Hospitality, Engineering with some of the leading blue chip companies in the region. He is currently the Head of Cybersecurity Policy and Standards with the Ministry of Transport and Communication.