PAKISTAN'S CYBER SECURITY CHALLENGES & SOLUTIONS

WHITEPAPER

Nahil Mahmood

7/21/2019

This paper characterizes a unique pattern of five (5) cyber security challenges prevalent in almost all of Pakistan's industry & organizations, expounds the contributing factors, and proposes solutions in the form of original cyber security models to address Pakistan's pressing cyber security challenges.

Contents

i. Table of Figures

ii. Executive Summary

Pakistan has witnessed a sharp surge in cyber attacks in the last 2 years in the areas covering ransomware, VoIP attacks, defacement of organizational websites, invoicing fraud, ATM skimming, SMS fraud, identity theft, online banking fraud, and data theft & manipulation. This paper examines the cyber security posture of Pakistan's organizations and government entities, and proposes solutions to address challenges.

Pakistan's cyber security implementation has been largely ignored for the last decade and sprawling IT networks across the country have almost entirely been erected without the consideration of cyber security protection as per International best-practices.

In fact, Pakistan's cyber security posture across the country follows a strikingly similar pattern characterized by the factors listed below:

i. Reactive
ii. Superficial
iii. Box-Approach
iv. Contentious
v. Governance-overkill

To enhance and improve the organizational security posture of Pakistan which is one-generation behind in security implementation, is an arduous but not an impossible task. The Cyber Security Transformation model, and the Cyber Security Transformation Matrix (CSMM) have been proposed in this whitepaper as practical solutions which are not limited to concept-only, but have been tried and tested in real security projects for various sectors in Pakistan.

While addressing the security challenges, it is pertinent to place the most emphasis where it has been lacking: in the grass-root and fundamental security practices such as security hardening and vulnerability management. Although these two practices or activities are widely accepted globally as foundational steps of the security effectiveness ladder, they are still being ignored to a great extent in Pakistan.

In order to fix a problem, the root cause must first be identified and the solution proposed accordingly. Unfortunately, players in Pakistan's security ecosystem such as regulators, security vendors, security services firms, and the organizations themselves are still not making an effort to identify and address the fundamental and obvious shortcomings.

Diligently following the Cyber Security Transformation Model and Cyber Security Maturity Matrix (CSMM) are the only way to address Pakistan's significantly dilapidated security posture which poses a national security risk, especially through security weaknesses of the critical infrastructure.

I. PREAMBLE

Cyber security attacks have registered a sharp increase in Pakistan over the last 2 years. The attacks have covered a broad spectrum hitting private organizations such as mobile operators & banks, the government, and private citizens. There has been much evidence of this surge in attacks in the national media covering[1] ransomware[2], VoIP attacks, defacement of organizational websites[3], invoicing fraud, ATM skimming, SMS fraud, identity theft, online banking fraud, and data theft & manipulation. The most prominent recent attack that has served as an "eye-opener" and a decisive rebuttal to those still in denial of Pakistan's weak cyber security posture was the Bank Islami cyber attack in November, 2018[4].

This paper specifically addresses weaknesses in Pakistan's organizational cyber security posture related to private and government organizations. Much of these organizations collectively constitute critical infrastructure[5]which are susceptible to cyber security attacks resulting in potential harm to national security[6], economic stability, and well-being of the citizens.

Whereas national cyber security strategy & structure, plus citizen-focused cyber security are also two additional important subjects, these will be addressed in future separate whitepapers in order to retain the focus of the existing whitepaper on Pakistan's cyber security challenges & solutions for Pakistan's organizations and government entities.

II. THE CHALLENGE

In order to propose adequate solutions, it is imperative to first accurately identify and understand Pakistan's cyber security challenges. Based on the author's exhaustive experience of cyber security consulting & implementation with all types and sizes of organizations in Pakistan over the last decade, the following may be characterized as key challenges of cyber security in the country. It is interesting to note that almost all organizations in Pakistan were found to be following a strikingly resembling pattern of weak cyber security posture, irrespective of geography, company type, or size.

Weak Cyber Security Posture - Challenge	Description Of Challenge
A. Reactive	Cyber security found to be reactive focused on "putting out the fire." Lack of a proactive, comprehensive and grass-roots security program
B. Superficial	Cyber security program lacking depth, understaffed, and in many cases found to be cosmetic limited to satisfying fleeting compliance requirements
C. Box Approach	Industry vendors driving "security box solution" as a silver bullet for every challenge, resulting in over-emphasis on appliance/box approach

[1] http://www.nr3c.gov.pk/crimecategorie.html
[2] https://arynews.tv/en/ransomware-infiltrates-computers-pakistans-govt-owned-insurance-company/
[3] https://tribune.com.pk/story/1481375/indian-hackers-deface-govt-websites-country-marks-independence/
[4] https://www.pakistantoday.com.pk/2018/12/21/bankislami-lost-6m-within-23-minutes-in-cyber-attack/
[5] See https://www.dhs.gov/cisa/critical-infrastructure-sectors
[6] https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks

D. Contention	Departments surrounding IT within the same organization such as Risk, Compliance, Security, and IT Audit carry a divergent view of what constitutes a secure organization. Lack of consensus on a common vision of what steps need to be taken to improve cyber security result in wastage of time and resources
E. Governance & Documentation Overkill	Cyber security efforts and initiatives found to be academic, with voluminous policy and procedures documentation existing in almost every organization, with actual implementation not exceeding 5-10% of the approved policy in almost all cases

Figure 1: Pakistan's 5 Cyber Security Challenges

The above five characteristics are ubiquitous throughout Pakistan from a cyber security posture perspective, with the only exception being the larger banks and telecoms organizations where more sophisticated staffing and enhanced spending improved on the national pattern by a mere and disappointing 10-15%. In fact, the larger banks and telecoms organizations possess a sizeable IT infrastructure and any gains in sophisticated staffing or spending are neutralized by increased attack surface resulting from more vast & complex IT infrastructure.

Pakistan's cyber security challenges may be summarized in this statement: there has been denial of cyber security in Pakistan over the last decade as organizations have erected their IT infrastructure with security as an after-thought. Hence cyber security in Pakistan lags one generation (about ten years) behind IT in terms of implementation.

Unfortunately, these challenges are persisting due to continued denial and attempts to make up for the lost-time by automated half-measures. The industry is looking for another silver bullet to cover for the lack of grassroots cyber security controls, that were never implemented.

III. CYBER SECURITY POSTURING

The easiest way to avoid a problem is to deny that the problem exists in the first place. As cyber security has been largely ignored in Pakistan over the last decade due to a lack of awareness, today's senior and powerful CIOs, IT Heads, Directors of IT Strategy and the Board are not willing to accept the bitter truth that their networks lack the most basic and fundamental cyber security controls as per International best-practices. So they conveniently deny that a problem exists.

To defend themselves and to convince the Board that the organizational cyber security posture is in good-standing, we have our worthwhile IT Audit commercial firms who will churn out an alphabet soup of IT audit observations in the form of an IT Risk Assessment (ITRA). These highly ineffective third-party IT Audits conducted by large international financial audit firms who invariably lack adequate cyber security domain knowledge have been continuing for more than two decades in Pakistan with the result that we are still struggling with the basic fundamentals of cyber security.

There are yet more culprits who have caused damage. The industry has misused the "penetration test" to the extent that it is considered the only cyber security check required to secure a new web portal or service. Security efforts in the form of a Secure-SDLC (secure software development life-cycle) are too

often completely ignored, and all hopes are pinned on a last-gasp penetration test to prove that the new business application meets security thresholds. Unfortunately the penetration test is a temporary and partial security assessment, and cannot be a replacement for a comprehensive security program.

International cyber security certification bodies that are focusing on governance are having a field day making fortunes off individual certifications that emphasize and prioritize academic risk management practices and security governance, thus adding to the problem. Although these international governance-focused cyber security certifications enjoy a reputable position in the mature IT markets of the western-world, they are counter-productive in an immature cyber security market like Pakistan where the fundamental cyber security measures are non-existent, and where there is already a "governance over-kill" at the expense of effective grassroots cyber security controls.

Pakistan's universities are churning out thousands of software professionals every year who join the industry as software developers. Software development is driving automation, ease of doing business, and government services outreach in all parts of the world, hence its importance cannot be over-emphasized. Unfortunately Pakistan's software professionals receive negligible training in software development security (Secure-SDLC) while in University. The result is obvious. Invariably, software developed in Pakistan does not meet the basic provisions of cyber security, resulting in consistently insecure applications. Again, a penetration test is considered the savior.

Effective sector regulators are almost non-existent in Pakistan. Around the globe, sector regulators play a crucial role in ensuring cyber security effectiveness through clear laws and strict enforcement. Apart from the financial sector, we are yet to come across a sector regulator in Pakistan who is cyber-security-conscious. Take telecoms, power & energy, health, retail, & government sectors…all of them lack comprehensive cyber security regulations and enforcement. Unfortunately the financial sector cyber security regulation has also been marred by severe deficiencies for decades; hence the resulting shocking level of cyber security posture & protection in Pakistani banks. The next section will highlight some of the fundamental and basic cyber security controls and activities which are missing in organizations belonging to all sectors in Pakistan.

IV. GLARING OMMISSIONS

Although an organizational cyber security program and its affiliated activities cannot be over-simplified, there are widely accepted basic and fundamental cyber security controls that cannot be denied in any security program. The first of these is security hardening. All Information Technology (IT) components run software at the core, and the software manufactured by vendors is available in default insecure configuration. End-users are expected to configure the IT devices or software customized to their specific requirement, and to tune the factory insecure settings through "security hardening." This comprises of shutting off extra ports and services, and implementing other controls and activities such as access control, and configuring the operating kernel or registry in a defensive posture to avoid being susceptible to malicious attacks, viruses or malware.

Security hardening as a practice was found to be either completely absent in Pakistan's organizations, or implemented at a very superficial and inadequate level, not following rigorous international best-practices such as the CIS Cyber Security Benchmarks[7]. Again, IT staff and CIOs are in denial that this basic grassroots cyber security measure is required as a foundational cyber security discipline, as the organizational IT infrastructure has now grown to a unmanageable size – all without effective hardening, and unfortunately "on their watch." Security hardening is hard and tough work and the easiest time to implement these security controls is when the infrastructure is being erected – not after it has been running without security hardening for the last 5-7 years, as the impact on production networks is substantial.

The second fundamental security practice widely accepted globally and in fact, unchallenged as a foundational cyber security measure is "vulnerability management." Again, there is a disconnect in Pakistan's cyber security landscape. There is an overwhelming emphasis on investing heavily in outrageously expensive appliances and "box solutions" promoted by security vendors as indispensable security protection and the "the silver bullet" for security effectiveness, whereas the most basic and foundational globally accepted security practices such as vulnerability management are overlooked altogether.

The international best-practice in mature IT markets is a vulnerability management lifecycle of one week[8] (7 days). That would entail scanning all organizational IT assets (all servers, computers, network devices, and other IT equipment such as printers and security cameras) through a commonly available vulnerability scanner every seven (7) days, and fixing all (or almost all) the vulnerabilities in that cycle of 7 days, only to repeat the cycle again. In Pakistan, the practice was found to be either non-existent, or glaringly deficient. Many banks do not have a vulnerability management internal capability, and outsource vulnerability management to external third-party vendors to conduct once a year, and that too driven by (inadequate) regulatory stipulations.

Vulnerability management has been ignored in Pakistan by IT teams for decades. As a result the tight security patching discipline required to maintain a secure IT infrastructure is years behind. Again, CIOs and IT teams are averse to admitting that this foundational security measure was either ignored in the past or is deficient now. Regulators are not demanding and enforcing a tight vulnerability management practice either, as per international benchmarks. Hence the denial continues, the disconnect widens, and with every passing day we are only worse off in security posture.

Where an impassioned effort has been made by a CIO, or by a Chief Information Security Officer (CISO), to initiate a vital across-the-board security hardening and vulnerability management program, it has been shot down by the Board as unnecessary, the resources have not been provided, or the Board has pushed the IT and security teams into more of the vicious circle characteristics we are already suffering from. An irrelevant and attention-diverting IT Risk Assessment (ITRA) from the Big-Four Audit firms

[7] https://www.cisecurity.org/cis-benchmarks/
[8] https://www.cisecurity.org/controls/continuous-vulnerability-management/

doesn't help, as the customer organization is rarely provided with a practical roadmap to actually improve cyber security of the organization.

Considering that approximately 70% of all organizations in Pakistan do not even possess or use a vulnerability scanner (a basic tool available for free[9] or for cost based on extent of the IT network to be scanned), it is safe to assume that at least that percentage of organizations (70%) do not have an established vulnerability management practice. In the security world, this is equivalent as an analogy to owning a house and trying to protect it without any walls, doors or windows.

V. THE SOLUTION – CYBER SECURITY TRANSFORMATION

After discussing at length the endemic cyber security challenges in Pakistan, it is pertinent to address the solutions, as merely pointing out defects holds no merit where improving the cyber security posture of the country is the objective.

In order to illustrate the solution to Pakistan's cyber security challenges, two models will be proposed in this section, which are not merely academic concepts but have been practically implemented by the author in a number of cyber security projects, spanning organizations belonging to several sectors such as financial, health care, industrial manufacturing, textiles, retail, and utilities.

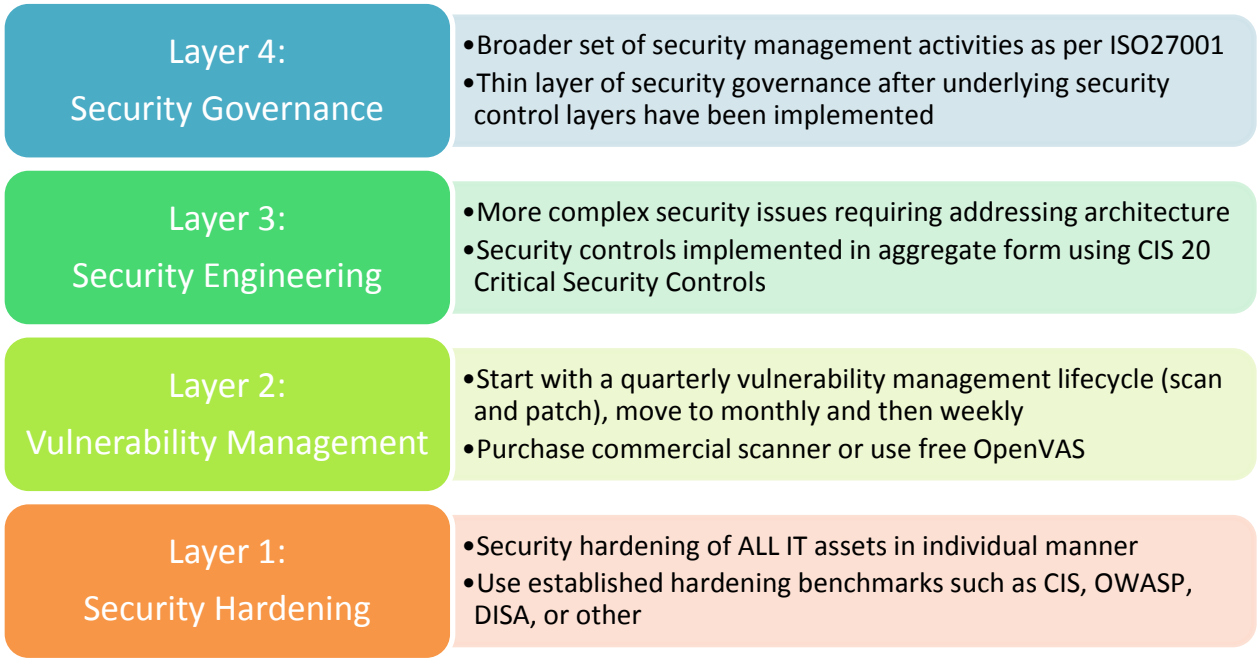

Figure 2: 4-Layer Cyber Security Transformation Model

The 4-layer Security Transformation Model shown in Figure 2 above, has been designed to specifically address Pakistan's cyber security challenges (implemented in a bottom-up manner). Pakistan's industry and government organizations severely lack effective and disciplined practices for security hardening

[9] http://www.openvas.org/

and vulnerability management. Hence, these activities fit into the first two layers of the proposed model, to be addressed as a priority.

In an environment where security staffing, spending, and focus has all been severely curtailed in the last decade, it is imperative to set the priorities clearly so that limited security resources directed at the Security Transformation program may be expended where they are most needed.

The Security Transformation model is implemented bottom-up, where the first two layers are categorized as essential low-hanging fruit as there is a clear target to address the critically missing hardening and vulnerability management for all IT assets. The typical Security Transformation program will take approximately 12-18 months depending upon the size of the organization and the experience and skill of its IT resources.

Once the first two (bottom) layers are either completed or momentum in implementation is satisfactory, the third layer (Security Engineering) is initiated about midway through the 12 month or 18 month Security Transformation project. The Security Engineering layer addresses security for IT assets in an aggregate manner through a framework such as CIS 20 Critical Controls[10] (e.g. controls for separate management VLAN to manage security of all servers in a single datacenter), whereas the first layer[11] addresses security hardening for individual IT assets (e.g. shutting down ports for one server). The third layer also addresses more complicated and complex security challenges related to security architecture, server placement, traffic flows, data protection, and the like; the motivation being to address the obvious low-hanging fruit in the form of first two layers of the model before attending to more complex security implementation belonging to the third layer.

Finally after the first three (bottom) layers of the Security Transformation model have been adequately implemented, it is time to address the security governance in the form of the fourth and top layer in order to culminate the program. The justification for the security governance being at the end of the Security Transformation program is two-fold. First of all, excessive documentation and academic governance in the absence of essential underlying controls is already characteristic in Pakistan, hence we do not want to worsen the existing problem. Second, it is more practical to "manage or govern" security, and direct energy in that direction once there are security controls already implemented to manage. Otherwise what are we managing ? The implementation of "top-down" governance driven cyber security has already failed miserably in Pakistan, otherwise we would have had rock-solid cyber security of organizations in the country, with strong security hardening and mature vulnerability management disciplines already in place.

The key factor to appreciate in order to justify the sequence of the Security Transformation model is to understand "what controls are critically missing, and what needs to be prioritized in order to best utilize limited resources and budgets ?" The Security Transformation model is a tailor-made solution to address Pakistan's unique and specific cyber security challenges.

[10] https://www.cisecurity.org/controls/
[11] https://www.cisecurity.org/cis-benchmarks/

VI. SOLUTION TO DIVERGING VIEW OF SECURITY: CYBER SECURITY MATURITY MATRIX (CSMM)

Here let us identify and address another pertinent challenge in the country which may also be categorized as a major contributing factor to Pakistan's rather poor cyber security implementation. There is a diverging view and lack of consistency in understanding of "what constitutes security."

As a fallout from the huge security effectiveness void left due to a decade of security indifference, vested organizations have all tried to fill the vacuum with their own version of "effective cyber security." Security training and certification bodies[12] have pushed security governance certifications which don't help solve Pakistan's security predicament, the large auditing firms have pushed their template-based alphabet soup of confusing IT Audits and Risk Assessments which are not geared to improving organizational cyber security posture, the security vendors have pushed appliances and boxes as silver bullets to solve every security problem (often without adequate configuration and customer training), security services companies have extolled the penetration test as an adequate security answer to every security challenge, and the regulators have either been asleep altogether, or in the case of the financial industry have been highly ineffective in ensuring the fundamental security foundations are in place.

As a result there is confusion in the industry in terms of "what to do to achieve cyber security," or what is cyber security?" With the limited resources that are going to be allocated for cyber security implementation it is imperative that the sequence of measures is given due consideration. The correct measures in the wrong sequence or dosage will only add to the existing problems.

The Cyber Security Maturity Matrix (CSMM) shown in Figure 3 (below), has been developed by the author of this paper in order to resolve the challenges listed above. It aims to categorize the levels of an effective cyber security program through a sequential series of six stages. Each stage requires specific and measurable security actions which are auditable and certifiable. Thus an independent (internal or external) body such as a Cyber Security Certification Board (CSCB) may be able to conduct practical onsite audits to verify that the organization has achieved the specific and measureable steps required to achieve a particular certification stage: Foundation, Fundamentals, Hardened, Protected, Monitored, and Secured.

The basic premise of the Cyber Security Maturity Matrix (CSMM) is that you can't improve what you can't measure, and that effective security has to follow an ordered, proactive, structured program, rather than a haphazard, reactive undertaking. The Cyber Security Maturity Matrix (CSMM) shown in Figure 3 (below) should be adopted by Pakistan's government, regulators, and industry organizations as an effective, sequential, certifiable model to standardize security implementation.

Specifically, if all the steps of the lower stage of the matrix are not fully achieved, the actions associated with a higher stage are quite meaningless, irrelevant, and counter-productive. The Cyber Security Maturity Matrix (CSMM) thus ensures that the practical basic foundational steps are all fully implemented in a sequential manner before more advanced and more expensive (often unnecessary)

[12] ISACA cyber security governance certifications

higher layer security actions are deployed. It also does not help to jump several layers of the model to try to implement more glamorous and automated technology solutions when the manual & essential (unfortunately laborious) steps belonging to lower layers have not been addressed.[13]

In order to do justice to the security vendors, the first two lower layers of the Cyber Security Maturity Matrix (CSMM) propose an Next-Generation (NGN) Firewall at the organizational perimeter with web filtering, email security, and anti-malware features. The third layer proposes an NGN Firewall at the entrance to the data center (also a prominently missing security characteristic in Pakistan). The higher layers (layers five and six) propose advanced security solutions only after the essential lower-level controls and essential security features have been put in place.

This again highlights the importance of correct sequence and dosage (intensity) while trying to solve a security problem. Pakistan's industry has had a largely lop-sided implementation sequence: turn the Cyber Security Transformation model, and Cyber Security Maturity Matrix (CSMM) upside down, and that will depict our industry's deficient security implementation trajectory.

Case in point: our industry is currently scrambling to enroll security vendors for advanced security solutions, and when you take a peek inside the organization to examine the most basic vulnerability management & patching practice, it would be embarrassingly deficient with large gaps in implementation and discipline (if it exists in the first place).

[13] http://www.deltatechglobal.com/solution-to-pakistans-security-challenges-cyber-security-maturity-matrix-csmm/

SECURITY MATURITY LEVEL	SECURITY POSTURE	MINIMUM CHARACTERISTICS
6. SECURED	Enterprise IT is secured through advanced security measures: threat simulation, protection & security orchestration; tested through Red Team exercises.	6.4 Red Team Penetration Testing
		6.3 Security Orchestration, Automation, & Incident Response
		6.2 Threat Protection
		6.1 Threat Simulation
5. MONITORED	Enterprise IT is monitored with centralized SOC,incident detection & response, plus data protection features such as DLP & encryption.	5.4 Security Operations Center (SOC) Implementation
		5.3 Critical Data Encryption
		5.2 Data Loss Prevention (DLP) Solution
		5.1 SIEM Solution For Security Events Detection
4. PROTECTED	Enterprise IT is protected with CIS 20 Critical Controls, software security code reviews, and pentesting; all topped with 27001 governance certification.	4.4 ISO27001:2013 (ISMS) Certification
		4.3 External/Internal Penetration Test (Critical Assets)
		4.2 Software Source Code Review For Critical Applications
		4.1 CIS 20 Critical Security Controls
3. HARDENED	Infrastructure & software hardening is in place using CIS or other accepted benchmarks, DC FW filtering, and tighter monthly VM practice is in place.	3.4 Software Security Hardening Program
		3.3 NGN FW At Data Center Entry Point With Filtering
		3.2 CIS Security Benchmarks Hardening Of All IT Assets
		3.1 Min Monthly Credential Based VM Cycle
2. FUNDAMENTALS	Security fundamentals including disciplined min quarterly vulnerability scanning practice plus edge NGN FW (with malware filtering) are in place.	2.4 Network Segmentation With VLANs By Dept/Service, & DMZ
		2.3 Edge NGN FW With Web, Email, Anti-malware Filtering
		2.2 Min Quarterly Credential Based VM Cycle
		2.1 Licensed Or Open Source VM Tool
1. FOUNDATION	Basic security foundational measures are in place such as licensed or open source OS, enterprise AV, AD & edge FW.	1.4 Edge FW With Filtering
		1.3 Active Directory (WS/S)
		1.2 Licensed Enterprise AV (WS/S)
		1.1 Licensed Windows OS (WS/S) Or Open Source

Figure 3: Cyber Security Maturity Matrix (CSMM)

It is also pertinent to note that the lower four (4) layers of both models proposed above, namely the Cyber Security Transformation Model (Figure 2), and the Cyber Security Maturity Matrix-CSMM (Figure 3) correspond to each other, and may be used in conjunction with each other.

To readers of this whitepaper who may still be in disbelief after learning of the significant gap in cyber security effectiveness in Pakistan, please consider that the very first step of the CSMM (Control 1.1: Licensed Windows Operating System or Open Source) is a severe challenge for Pakistan's SMEs and also for many large organizations. While Microsoft is justified in selling its licensed operating system for servers and workstations, organizations in Pakistan are averse to paying high recurring licensing costs, and more than half of Pakistan's industry is collectively using pirated software. Pirated operating system software is widely accepted to be infested with malware, and is a mis-step in the cyber security journey. There is nothing stopping an organization from using open source software for their workstations and servers. Enter software vendors who are adept at marketing expensive software, and the lack of initiative of our industry to develop an open source software eco-system which is highly cost-effective.

VII. SECTOR SPECIFIC NATIONAL SECURITY RISKS

There are other cyber security considerations relevant to specific sectors which pose a direct threat to national security. One of these areas is SS7 Signaling Security relevant to the mobile operators. It is now widely known[14] that the basic signaling system (SS7 for GSM 2G/3G and Diameter for 4G) used by mobile network operators has security vulnerabilities which may be easily exploited by an attacker.

Common attacks resulting from SS7 and Diameter signaling vulnerabilities as researched by Positive Technologies[15] are:

- IMSI disclosure
- Discovering any subscribers physical location
- Disrupting subscriber service
- Intercepting SMS messages
- Intercepting outgoing calls
- Redirecting incoming calls

All of the above attacks are possible by an attacker easily penetrating the mobile operator network through International roaming[16]. Unless specific actions are taken by all mobile operators as per GSMA security recommendations, the mobile network is a high-risk for national security.

Similarly, the Industrial Control Systems (ICS) and SCADA systems belonging to power generation & distribution companies and the Oil & Gas sector need to be secured with the help of IOT and OT (Operational Technology) security measures relevant to the specific industry and sector. In recent global cyber attacks, the national utility grid has either been compromised or attacked[17], making it a susceptible target in cyber warfare.

In fact, all sectors forming the critical infrastructure such as financial, telecoms, energy, utilities, and government sectors possess very specific cyber security risks unique to their technology and infrastructure.

Here it is pertinent to mention the role of a National Cyber Security Agency in Pakistan (NCSA) which sits at the pinnacle of the cyber security hierarchy, and may direct specific regulators to take industry-specific security measures to ensure that the country's critical infrastructure security exposure is minimized.

[14] https://www.ptsecurity.com/upload/ptcom/SS7_WP_A4.ENG.0036.01.DEC.28.2014.pdf
[15] https://www.ptsecurity.com/ww-en/
[16] https://www.ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/
[17] https://www.bbc.com/news/technology-48675203

VIII. CONCLUSION

Pakistan is significantly behind in ensuring a robust cyber security posture of its organizations and government entities. This poses a significant risk to critical infrastructure, and hence to national security.

It is pertinent to mention that we do not need to re-invent the wheel while finding a solution to Pakistan's cyber security posture improvement. Cyber security is a widely adopted practice internationally just like dentistry and law, and there is a sufficient pool of best-practices, frameworks, research and case studies that we may follow to our advantage.

The first step in effectively addressing cyber security improvement is to accept that the fundamental practices such as security hardening and vulnerability management are imperative and a priority, and unfortunately largely absent in Pakistan.

A National Cyber Security Agency (NCSA) must push these fundamental sector specific requirements down to regulators, who in turn are obligated to enforce cyber security best practices in Pakistan's organizations and government. The cyber security myth must be shattered by proposing and publishing practical and beneficial Pakistan-specific security frameworks such as the Cyber Security Maturity Matrix (CSMM). The Cyber Security Maturity Matrix proposes specific technical measures in each of its six layers to ensure cyber security is measurable, transparent, and auditable.

In order to ensure that the security posture actually improves (rather than continuing to hide behind misleading documentation and unhelpful IT Audit and Risk Assessment reports), there is a need to establish a Cyber Security Certification Board (CSCB) that may actually conduct onsite security assessments of important organizations part of the critical infrastructure to categorize, rate, certify and publish security posture against the Cyber Security Maturity Matrix (CSMM).

The next paper in this series will address Pakistan's international cyber security standing as per the ITU Global Cyber Security Index[18] 2018 report, and recommendations for a national cyber security strategy and structure for Pakistan.[19]

[18] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf
[19] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

About The Author

Nahil Mahmood has over 21 years experience in IT and the last 12 years specifically in cyber security implementation & consulting. He was the CISO at one of the largest commercial banks of Pakistan, and was awarded the ISC2 Asia Pacific Cyber Security Leadership Achievement Award (ISLA) in 2012 in a ceremony in Tokyo, Japan for his contribution to cyber security enhancement in Pakistan. For the last 7 years he has been CEO for Delta Tech (http://www.deltatechglobal.com), one of the leading cyber security consulting firms in Pakistan. At Delta Tech, Nahil has worked on over 50 cyber security projects in all major cities of Pakistan with all types and sizes of Pakistani organizations, providing him a unique insight into the nature and extent of Pakistan's pressing cyber security challenges.

Nahil speaks at the leading cyber security conferences in Pakistan, and writes frequently on cyber security improvement for the country; a topic about which he is passionate. As a cyber security thought leader, he has also characterized Pakistan's cyber security challenges, and developed original and tailor-made frameworks to address Pakistan's cyber security challenges (such as the Cyber Security Transformation Model and Cyber Security Maturity Matrix-CSMM).

Nahil has held the prestigious CCIE R&S (2008-2012) and CISSP (2012-2015) certifications in the past, and was also Founder & President of Cloud Security Alliance in Pakistan (2012-2015). He has officiated and presented cyber security papers at National Defence College (NDC), and for various government cyber security working groups. Moreover, he also provides security training to the government of Punjab, and has worked with SBP and PTA to provide specialized security training to the respective industry sectors.

In October 2019, his comprehensive online course titled "Information Security Transformation – CS205" will become available for free viewing and enrolment via the Virtual University of Pakistan. This course comprehensively covers the Cyber Security Transformation methodology for improving Pakistan's cyber security posture.

He can be reached at: nahil@deltatechglobal.com or nahil@deltatechglobal.net.