



OOOPS.
YOUR
FILES
HAVE
BEEN
ENCRYPTED!

RANSOMWARE

**RANSOMWARE
ENCRYPTION
MECHANISMS**



BGD e-GOV CIRT

MONTHLY MAGAZINE

October 2020

**Traditional VAPT VS Effective
Security Assessment Program**

**Importance of Cyber Security
Incident Management**



BGD e-GOV CIRT



| | |
|----------------------|---|
| Name of Magazine | Bangladesh Cybersecurity Magazine |
| Chief Patron | Zunaid Ahmed Palak Hon'ble State Minister for ICT |
| Chief Advisor | N M Zeaul Alam Senior Secretary, ICT Division |
| Chief Editor | Tarique M Barkatullah Project Director |
| Magazine Mode | Monthly |
| Issue | October 2020 |
| Published From | BGD e-GOV CIRT, Bangladesh Computer Council, ICT Division, Ministry of Posts, Telecommunications and Information Technology |
| Address | E-14/X, ICT Tower, Agargaon, Dhaka- 1207, Bangladesh |
| Contact | info@cirt.gov.bd |
| Content Provider | BGD e-GOV CIRT Team |
| Content Finalized by | Tarique M Barkatullah, Project Director Tawhidur Rahman Pail, Team Lead |
| Content Designer | BGD e-GOV CIRT Team |
| Image Content | From Internet |
| Graphics Content | From Internet |
| Copyright | All rights reserved |

Contents

| | |
|---|----|
| Ransomware Encryption Mechanisms..... | 1 |
| Introduction..... | 1 |
| Cryptography 101..... | 1 |
| How ransomware effects..... | 3 |
| Vulnerability in ransomware | 4 |
| Conclusion..... | 5 |
| BGD e-GOV CIRT has successfully organized country's First Cyber Drill 2020 | 5 |
| BGD e-GOV CIRT holds Bangladesh's first-ever cyber drill | 8 |
| Awareness for Spam E-mail | 9 |
| A Comparison of Global Data Localisation Policies and Frameworks..... | 18 |
| Introduction..... | 18 |
| An overview of data localisation | 19 |
| Pros and Cons of Data Localisation..... | 19 |
| Strictness of approach to Data Localisation..... | 21 |
| Explicit and Implicit Measures..... | 22 |
| Global data localisation laws | 24 |
| Summary Analysis..... | 36 |
| Conclusion..... | 38 |
| Traditional VAPT VS Effective Security Assessment Program For Enterprises | 39 |
| Things to know about Security Intelligence..... | 46 |
| WSIS Prizes 2020 - SUCCESS STORY | 50 |

Ransomware Encryption Mechanisms

Rezaur Rahman, Incident Handler
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Introduction

Ransomware is a kind of malware which cryptographically lock user files and prevent them from accessing. As content of the affected files are changed, it becomes unusable for the user. To use these files again, the attacker claims financial benefit, usually in BitCoin, and in return the decryption key is promised to be provided and with which the user will be able to perform decryption and eventually convert the files back to readable format.

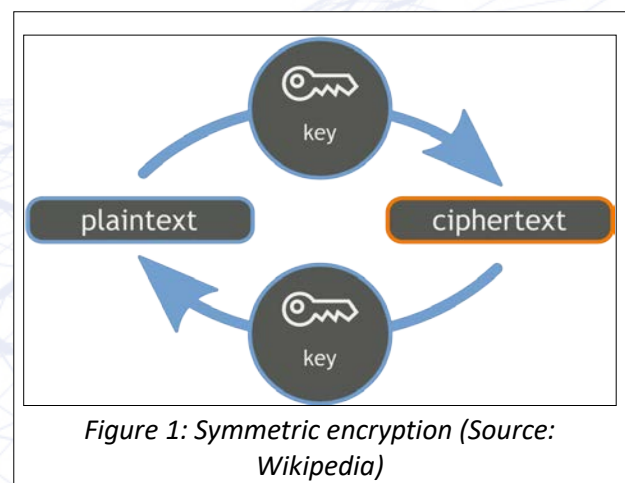
But to understand how a ransomware works, first some basic knowledge in cryptography is required and an overview is given below.

Cryptography 101

In this section, we will briefly discuss on how a encryption mechanism works and how it is used by the malware. After which, we will be able to understand at a basic level that whether we can decrypt the affected files or not.

Symmetric Key:

This encryption mechanism is dependent on a specific key. A mathematically computational process is performed on the data to change it with the help of the key and reverse process is applied to revert it back to original form. This key is used to both encrypt and decrypt content of a file. This key can be considered as a lock with which you secure your personal items and those who have the key can unlock and obtain the those items. The process is illustrated in Figure 1.



This key can be any thing from numbers to symbols at any combination. The length of this key is not expected to be short so that it can not be brute forced. For those who are not familiar with brute force, it is a process by which all the character combinations are tested to discover the password.



There are many algorithms which we can use to encrypt our data securely.

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

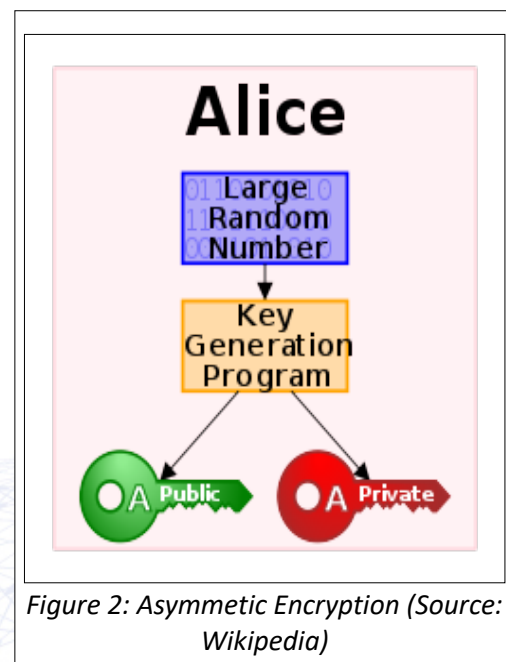
One of the primary problem with is method is the key itself. It is quite difficult to either transport this key from one location to another, or store it securely. Such encryption method does not provide any inherent ability to protect the key from outsiders. If the key is obtained by another person, he or she can use this key to unlock the data with ease.

However the performance benefit of this encryption mechanism is high. The data can be encrypted or decrypted extremely fast. If a user want to encrypt a large pool of data, the user will see significant reduction of time when comparing with asymmetric encryption.

Asymmetric Key:

Asymmetric cryptography is also known as public-private key encryption. The

public key in this mechanism is being used for encryption and the private key is for decryption. By randomly generating one pair of public key and one private key, which are mathematically related, one of the key is used for encryption and another one is for decryption.



The primary advantage of this method is that the key can easily be transported. This is because with the public key, one party can only encrypt the data thus the recipient can send his or her public key anywhere with out any issue. As the only recipient has the private key, which is used for decryption, is never being disclosed, only that recipient can decrypt the sent data and view its content. Even if the public key is disclosed to an outsider, the attacker will not be able to view the content

because the attacker does not have the decryption key aka private key. Some of the common technologies are given below:

- Diffie-Hellman Key Agreement
- RSA (Rivest Shamir Adleman)
- ECC (Elliptic Curve Cryptography)
- El Gamel
- DSA (Digital Signature Algorithm)

How ransomware effects

Such malwares usually gains access using various methods. It can range from user running a pirated software obtained from the internet to malware itself invading the user's workstations by exploiting security holes. In many cases, they tend to use chain of cascading processes to gain foothold in the victim's workstation.

Anti-virus programs can help user to identify such programs but unfortunately, in many cases they are not taken seriously and users tend to ignore the notifications rather than to investigate and find out what might happen if actions are not taken immediately. This problem is exacerbated by users allowing software like cracks and keygens to run, overriding the anti-virus's recommended actions.

If the penetration is successful, the ransomware quickly tries to encrypt user files. System files and other critical

directories are ignored as if they are modified, the system will become inoperable.

In the next sections we will briefly look into the method which ransomwares use to encrypt user data.

Symmetric method:

The primary advantage of this method is the speed of encryption. As symmetric encryption is very fast, it gives users very little time to react after first detecting any abnormalities caused of the virus. But like any other symmetric encryption mechanism, the key to encrypt and decrypt is same thus if the key can be located, the process can be reversed and the original content can be obtained.

Since this key has to be stored somewhere in order to either continue the encryption process or perform decryption after receiving extorted amount, the key should be in decrypted state so that the process can continue. Researches can try to find this key and use it to decrypt user files to its original state.

Asymmetric method:

Using this scheme, a previously generated private and public key pair will be used and the public key, used for encryption only, will be hard-coded inside the malware. By this way any other decryption method is rendered impossible. Without the private key for



decryption, valued files of the user will be lost.

However, this method has its own problem as the private key of this process will remain same for every user it infects thus if a ransomware is paid, the attacker will have to release the key to ensure others continue to do so to recover their files but releasing the private key means it can be used to decrypt all other systems as well.

Hybrid method:

This method, from a ransomware's perspective, is one of the most effective way to render victims files unusable. The recovery mechanism is almost impossible as they use the speed of symmetric encryption and the security of asymmetric encryption thus making the whole system almost impossible to reverse engineer.

The simplified version of this method is, firstly the malware connects to a Command & Control (C&C) system over the internet to generate a public key and private key pair. As the public key is used to encrypt, it is transported to the end user and the private key is stored inside the control server.

If the above operations succeeds, the malware moves to the next phase of the operation. It should be noted that, if the key generation process is not successful, the malware does not take any further steps. The ransomware moves to next stage by generating a

symmetric key to encrypt the user files. It quickly encrypts users valuable files like personal photos or official documents and changes the extension of those files. As symmetric encryption method is fast and it targets specific file extensions, they usually perform their actions very swiftly and does not give users any chance to react.

And finally, when the malware finishes encrypting all the files, the symmetric key is encrypted using the public asymmetric key. All other traces of the encrypting symmetric key is now removed from the system making the author of the C&C server the only entity who can practically decrypt the user files.

Vulnerability in ransomware

All the algorithms are considered unbreakable but fortunately for us that the standards of those algorithms are not properly implemented inside the ransomware and consequently security researchers can take advantage of those security holes and make tools to decrypt the files.

Moreover, there are also some weaknesses which can be used against the ransomwares to make them unusable. Some of the key weaknesses which has been observed in real life scenario has been given below:

1. Any encryption method which has been created by the author of the ransomware can be reverse-engineered.



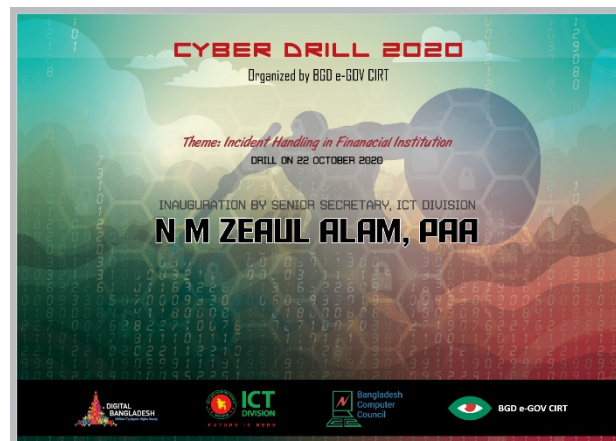
2. Storing the key in the victim's computer can be obtained.
3. Already vulnerable algorithms used by the ransomware can be exploited to gain the key.
4. Without the C&C server some ransomware does not function, thus taking those servers out from the internet can stop the infection.

Conclusion

As problems with ransomware has been discovered and exploited to gain the key and eventually to decrypt the files, more and more ransomwares are embracing more standard implementation of those algorithms thus making it more difficult to develop tools to decypher user files.

Thus obtaining files from valid sources and updating software in a regular basis must be enforced to make sure we can protect ourselves from such harmful software. Additionally, we all should keep ourselves aware of the danger and consequences if an attack happens and learn potential attack vector

BGD e-GOV CIRT has successfully organized country's First Cyber Drill 2020



BGD e-GOV CIRT has successfully organized country's 1st cyber drill on 22 October 2020. It was designed for the personnel of financial institutions. The purpose of this drill was to sharpen skills during incident handling. Challenges consisted of the use of hands-on skills, tools and real targets, real memory captures, and challenging analysis scenarios.

The theme for this event was "Incident Handling in Financial Institute". In Cyber Security, incident management is the process of identifying, managing, recording and analyzing security threats or incidents in real time. Total 35 teams from different types of organization including Banks & Non-Bank Financial institutions participated in the drill. We believe this drill helped them to build resilience and capacity for handling cyber threats in future.



BGD e-GOV CIRT Cyber Drill 2020 Scoreboard

| Team Name / Organization Name | Score | Position |
|---|-------|----------|
| NCC Bank Ltd | 85 | 1 |
| Pubali Bank Ltd. | 83 | 2 |
| Information Technology Consultants Limited | 76 | 3 |
| Bangladesh Bank | 70 | 4 |
| IFIC Bank Limited | 68 | 5 |
| Janata Bank Limited | 63 | 6 |
| BRACNet Limited | 58 | 7 |
| Bangladesh Commerce Bank Ltd | 58 | 8 |
| Cyberdefenders | 53 | 9 |
| National Telecommunication Monitoring Centre (NTMC) | 50 | 10 |
| The Premier Bank Ltd. | 48.5 | 11 |
| Bangladesh Development Bank Limited | 43 | 12 |
| Community Bank Bangladesh Limited | 43 | 13 |
| Uttara Bank Ltd. | 43 | 14 |
| The B Team | 33.5 | 15 |
| United Commercial Bank Ltd (IT Audit Team) | 28 | 16 |
| Mercantile Bank Ltd. | 21 | 17 |
| BRAC IT Services Limited | 12 | 18 |
| Ansar VDP Unnayan Bank | 10 | 19 |
| Investment Corporation of Bangladesh | 8 | 20 |
| United Finance Ltd_HA | 8 | 21 |
| Return Zero | 1 | 22 |
| Bangladesh police | 0 | 23 |
| Ansar VDP Bank Ltd. | 0 | 24 |
| BEPZA | 0 | 25 |
| Blue Team Bangladesh | 0 | 26 |
| Cybercrime Investigation Division, CTIC | 0 | 27 |
| Digital Security Agency | 0 | 28 |
| Emerging IT Bangladesh Limited | 0 | 29 |
| Mutual Trust Bank Limited | 0 | 30 |
| ONE Bank Limited | 0 | 31 |
| Rupali Bank Limited | 0 | 32 |
| TheCityBank | 0 | 33 |
| United Finance Limited_MH | 0 | 34 |
| United Finance Limited_RM | 0 | 35 |

Final Scoreboard URL: <https://www.cirt.gov.bd/drill-score2020/>



Fig: The Organizing Team of Cyber Drill

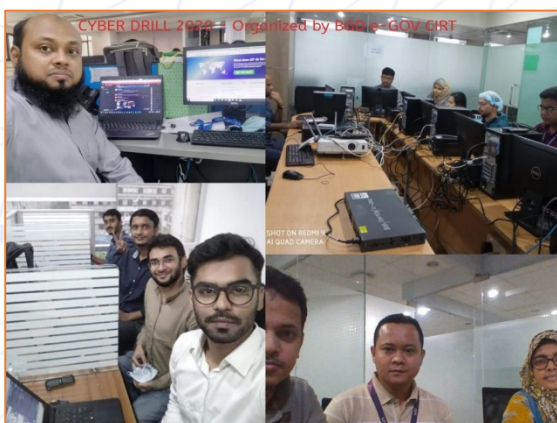


Fig: Participating Team

The cyber drill was inaugurated by Director General of Digital Security Agency, Md. Rezaul Karim and by Project Director of BGD e-GOV CIRT, Tarique M Barkatullah. Hon Col John Davies, Co-Founder & Chairperson of Cyber Wales gave a short presentation in the event. The event concluded on a high note by Executive Director of

Bangladesh Computer Council,
Mr. Parthapratim Deb.

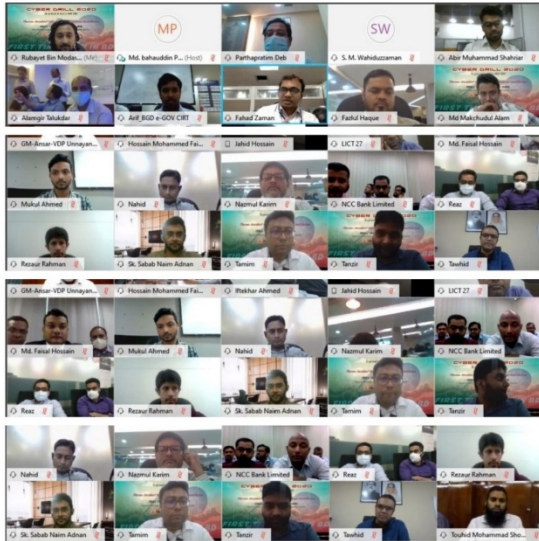


Fig: Online event of Inauguration

BGD e-GOV CIRT holds Bangladesh's first-ever cyber drill

FE ONLINE REPORT | Published: October 23,
2020 15:00:50



Bangladesh's cybersecurity platform
BGD e-GOV CIRT has said it on
Thursday organised the country's first
ever cyber drill.

A total of 35 teams from different types
of organisations, including banks &
non-bank financial institutions,
participated in the event, the cyber
security platform said in a press release
on Friday.

Designed for the personnel of financial
institutions, the drill aimed at
sharpening skills during incident
handling and building resilience and
capacity for handling cyber threats in
future.

The cyber drill, the theme of which was
"Incident Handling in Financial
Institutes", concluded on a high note. In
cyber security, incident management is
the process of identifying, managing,
recording and analysing security threats
or incidents in real time.

Director General of Digital Security
Agency Md. Rezaul Karim and Project
Director of BGD e-GOV CIRT Tarique M
Barkatullah inaugurated the event,
while Col John Davies, co-founder &
chairperson of Cyber Wales, gave a
short presentation there.



Awareness for Spam E-mail

Tahsina Shefat, Quality Assurance Manager
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

E-mail contain suspicious links, attachments, suspicious subject, unauthorized sender, unwanted subject is called Spam E-mail which could steal your valuable information from your E-mail accounts, even your PCs. For sending spam E-mails, your E-mail accounts are being used by the hackers. Hackers/ scammers breach your E-mail accounts in many ways to send these spam mails. Spam mail problem is a great threat for E-mail security. There is no E-mail user who is left untouched by spam. At present every E-mail user is affected and tired of seeing spam in his inbox every day. It's a big task clearing up. It's an unwanted E-mail message or



posting, commercial in nature, which is sent to multiple recipients and does not contain a valid output. Spam is commercial advertising, often for

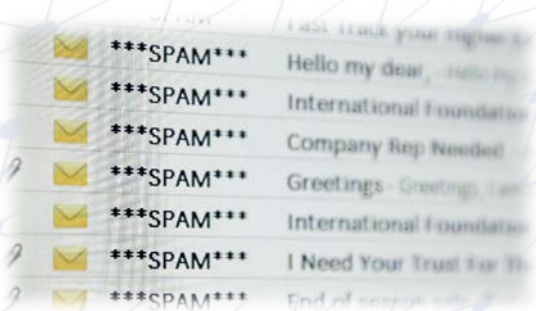
dubious products, get rich-quick schemes, or partially-legal services or pornography. Spam is the biggest disturbance today to E-mail users worldwide.

An unreliable person or a group of unreliable people, automated software developed to send unwanted messages in bulk through E-mail are known as spammers. Spammers could be individuals, e-marketers or malicious gangs organized into spamming networks. Spammers could also make spamming automated by making computers zombies with specially programmed scripts and viruses. The reason for receiving spam mails from spammers. Spammers spam basically to earn money through online marketing by inducing various products and services. General reasons for the spammers to spam: 1. malicious intentions – To disable recipient's E-mail account or server by sending bulk messages – spam attackers can paralyze servers or any individuals. 2. Online fraud leads to declaring the personal information like credit card number, phone number, bank account number for defrauding the recipient out of his/her money.



Types of spam

1. Sale of pirated software at lower cheap prices.
2. Fake health products and remedies.
3. Fake online pharmacies.
4. Stock offerings for unknown start-up ventures.
5. Advertisements and links to pornographic websites.
6. Pre-approved loans, insurance credit cards, credit reports, etc.
7. Fake online social hubs
8. Online gambling, astrology & casinos.
9. Online degree offers and fake real estates.
10. subjected as "Work from home", and "Become Rich Quicker", "Make Money Faster", "Hi", "Hello", "offer" etc.
11. Multi-Level Marketing schemes.
12. Chain letters with request for forwarding to others.



Analytical tricks for finding spam mail

After getting new mail in your inbox, the most important question you need to ask yourself that are

- Was I expecting an E-mail recently?
- Is this a person that would normally message me?
- Does the E-mail Subject seem suspicious or reliable?
- Does the sender give a valid reason for me to open this link?
- Is this a business I am subscribed to?
- The E-mail address and domain seems valid or invalid?

The E-mail system is designed with E-mail Security Gateway (ESG) to provide high availability e-mail service, increase the security of e-mail service, reduce the rate of spam in e-mail service, provide more user friendly e-mail service to customer, filters all E-mail traffic to protect organizations from E-mail -borne threats and data leaks but sometime Security port cannot able to block, filter or flag the mail as suspicious. Some spam mail also Contain valid subject which seems as valid mail with suspicious link. So it becomes compulsory to be conscious for using an E-mail account.

Aware with E-mail subject line: The E-mail's subject line is way to identify the spam E-mail. E-mail Recipient should be concerned about these categories:



- E-mail with Manipulative subject: creating unnecessary urgency or pressure.
- E-mail with Needy subject: sounding desperate.
- E-mail with messy subject: easily emotional hurt.
- E-mail with Cheap subject: no pre-qualifications.
- E-mail with abnormal subject: statements those are too good to be true.
- E-mail with Shady E-mail with: ethically or legally questionable behavior.

Aware for choosing your E-mail account password

Many times a hacker will not make the effort to create a new E-mail address. you can see a ridiculous address when you hover over the display name, indicating that the sender is an impostor. Sometimes the address will even be an almost identical address. Received messages from check and compare the addresses, signatures, and messaging style. All business E-mail s are sent during business hours. Nine to five is the general time period that an entity like a bank would send an E-mail. Unless the company is based in a different time zone, any company

messaging you late at night is likely a Spam mail. Do Not Take Chances with Passwords. The easiest way to become a victim of cyberattacks is to have a bad password. When it comes to passwords, rules for apply:

- Do not set flimsy passwords that are easily hack-able.
- Do not use the same password for all your online accounts.



- Change passwords regularly.
- Do not use date of birth
- Do not use pet name.
- Do not use spouse name
- Do not save passwords on browsers.

A strong password is a combination of numbers, letters, and symbols and avoid spelling out words which you are easily associated with. Use strong passwords for your accounts and. Change your password with a strong one for your security. Your password should be a combination of alphabets both capital and small letters (A-Z, a-z), numbers (0-9) and special characters (!, @, #, \$, %, ^, &, *). Change your E-mail account password every 3 months.



Be Aware with Sender's E-mail address

E-mail is still the most effective way for hackers to hit you with cyber attacks. Therefore, the first step here is to use a secure E-mail account that uses approved spam and malware filters. Additionally, you must remain vigilant against unknown senders and downloading unrecognized files which could contain all sorts of nasty viruses. Always check the sender address (not display name) with a unique domain and valid to understand if the mail is valid or not.

Aware with Unknown Links of E-mail

Cyber attacks occur is through links that hackers can send from recognized E-mail addresses. Be aware of E-mails from addresses within your contacts list that show up with just a random link. In this way they can execute malware programs which compromise your data. Ignore any mail saying "ACTIVATE YOUR ACCOUNT", "UPGRADE NOW", "TO ACTIVATE CLICK HERE", "QUOTA INCREASE", "ACCOUNT BLOCKED", "E-MAIL BLOCKED" or similar like these.

All these are SPAM MAILs which contain suspicious links. Don't click any of the links on those mails as the links can steal your valuable information.

Aware with grammatical mistakes in a mail

All hackers aren't very good at writing. Many of them are from non-English-speaking countries and from backgrounds where they will have limited access or opportunity to learn the language. It becomes a lot easier to spot the difference between a typo made by a legitimate sender and a scam. When creating Spam messages, hacker will often use a spellchecker or translation machine, which will give them all the right words but not necessarily in the proper context which could be suspicious E-mail. Always be logged out your E-mail account after work done.





Install a good antivirus program

Installing antivirus software is a way for minimizing the rate of spam E-mails reaching in your inbox. Patches find and fix vulnerabilities in your program may have.

Moreover, Spam E-mails will continue to evolve as long as humans continue to innovate and hunger for money. The last piece of advice is to trust your gut. If a company or friend is sending you an E-mail and something seems off about it, something is probably amiss. Before clicking any link, you can always call the company or a friend to confirm that they intended to send you a link. Keep yourself up-to-date when it comes to the newest scams and cyberattacks.

সাইবার সিকিউরিটি ইন্সিডেন্ট ও এর ব্যবস্থাপনার গুরুত্ব (Importance of Cyber Security Incident Management):

Md. Rezaul Islam, Quality Assurance Manager
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

প্রারম্ভিক (Introduction)

কম্পিউটার ইন্সিডেন্ট হল স্বাভাবিক ঘটনা থেকে ব্যতিক্রম কোন ঘটনা বা দুর্ঘটনা, যেখানে কম্পিউটার স্বাভাবিক আচরন করে না, এক বা একাধিক প্রোগ্রাম ঠিকমত কাজ করে না, ফলে কম্পিউটারের নিয়মিত কার্যক্রম ব্যাহত হয়। সাইবার ইন্সিডেন্ট হল, সাইবার স্পেসে সংঘটিত এমন দুর্ঘটনা, যা উদ্দেশ্যপ্রণোদিতভাবে ঘটিয়ে থাকে তার অসং উদ্দেশ্য সাধনের লক্ষ্যে। যেমন কোন কম্পিউটারে অনধিকার প্রবেশের মাধ্যমে সেখানে ডাটা চুরি করা, ম্যালওয়্যার ঢুকিয়ে দেওয়া, কোন ওয়েবসাইট হ্যাক করে বসিয়ে দেওয়া, কারো সুনাম নষ্টের উদ্দেশ্যে সাইবার স্পেসে তার ছবির বিকৃতি সাধন করা ইত্যাদি। আবার কেউবা সাইবার ইন্সিডেন্ট ঘটিয়ে থাকে নিজের অলক্ষ্য বা অজ্ঞতাবশত, যেমন কোন ক্ষতিকর প্রোগ্রামে বা ম্যালওয়্যারে ক্লিক করলেই তা কার্যকর হয়ে যায়, আবার আকর্ষণীয় নামের কোন ছবি বা সংযুক্তি ওপেন করলেই সেটা কাজ করা শুরু করে। তবে নিম্নলিখিত এক বা



একাধিক কারনও সাইবার ইন্সিডেন্টের অন্তর্ভুক্তঃ

- ভাইরাস/মালওয়্যার আক্রমণ করা
- ডিনায়াল অফ সার্ভিস আক্রমণ (DoS) করে ওয়েবসাইট বা এন্টারপ্রাইস সিস্টেম ডাউন করে দেওয়া
- অভ্যন্তরীণ সিকিউরিটি ইনফ্রাস্ট্রাকচার কোন কারনে ফেল করা
- সিস্টেম ফাইলসমূহ এনক্রিপ্ট করে রান্সম (Ransom) দাবি করা
- ফিসিং ইমেইল করা বা গুরুত্বপূর্ণ ব্যক্তির ইমেইল স্পুফিং (Spoofing) করা ইত্যাদি।



ইন্সিডেন্ট প্রতিক্রিয়াঃ (Incident Response)

সাইবার ইন্সিডেন্ট প্রতিক্রিয়া হল এমন সমন্বিত প্রক্রিয়া, যার মাধ্যমে কোন প্রতিষ্ঠান সাইবার দুর্ঘটনা প্রতিরোধ করে বা দুর্ঘটনার ফলে ক্ষতির মোকাবেলা করে। সাইবার স্পেসে সংগঠিত এই দুর্ঘটনার শুরু থেকে এর উত্তরন পর্যন্ত কিছু পর্যায়ক্রমিক, সামঞ্জস্যপূর্ণ

প্রক্রিয়া অনুসরণ করা হয়, যার মাধ্যমে সংগঠিত ঘটনার অদ্যপান্ত সংরক্ষণ করার জন্য অত্যন্ত গুরুত্বপূর্ণ। এর ফলে সাইবার ইন্সিডেন্টের মূল কারন চিহ্নিত করে, তার ফলে ক্ষতির পরিমান কমিয়ে এনে দ্রুত উত্তরন করে ও ভবিষ্যতে সমজাতীয় ঘটনার প্রতিরোধ সহজতর করে। এছাড়া আইনি পদক্ষেপ গ্রহন, তদন্ত, মূল অপরাধীকে চিহ্নিত করে ও বিচারিক প্রক্রিয়া ত্বরান্বিত ও নিশ্চিত করে।

কেন সাইবার ইন্সিডেন্ট ব্যবস্থাপনা প্রয়োজন (Why Cyber Incident Management Needed)?

বিশ্বব্যাপী সাইবার ইন্সিডেন্ট জ্যামিতিক হারে বৃদ্ধি পেয়েছে। প্রতিনিয়ত এর আকার, জটিলতা ও ক্ষতির পরিমান বৃদ্ধি পেয়েই চলেছে। এর ফলে সাইবার আক্রান্ত প্রতিষ্ঠানের আর্থিক, সম্মানের ক্ষতি, গ্রাহক কমে যাওয়া, কোম্পানির সময় ও সম্পদের অপচয় সহ ব্র্যান্ডের মূল্য খতিগ্রস্ত হচ্ছে। এসব ক্ষতির থেকে রক্ষা পেতে, ইন্সিডেন্টের পর ক্ষতির পরিমান কমিয়ে এনে যত দ্রুত সম্ভব পরিসেবা পুরদ্ধার করা ও ভবিষ্যৎ একই ঘটনার পুনঃরাবৃতি রোধ করতে সাইবার ইন্সিডেন্ট ব্যবস্থাপনা প্রয়োজন।

সাইবার ইন্সিডেন্টের ফলে সংশ্লিষ্ট ব্যক্তি/প্রতিষ্ঠান ক্ষতিগ্রস্ত হলে বাংলাদেশের বিদ্যমান আইনের সহায়তা নিতে পারেন। আইনি সহায়তা নিতে হলে অবশ্যই প্রতিটি ইন্সিডেন্ট যথাযথভাবে নথিভুক্ত এবং এর সাথে সংশ্লিষ্ট প্রমানাদি আদালতে উপস্থাপন

করা জরুরী। এছাড়া সাইবার ইন্সিডেন্ট ঘটলে ঘটনার প্রমানাদি সংরক্ষন করা (Containment), বর্ণনার ধারাবাহিকতা রক্ষা করা (Chain of Custody) এবং মূল কারন বিশ্লেষণ (Root Cause Analysis) করা এবং ইন্সিডেন্ট থেকে প্রাপ্ত শিক্ষা নিয়ে একই ঘটনার পুনরাবৃত্তি রোধ করতে সঠিক ব্যবস্থাপনা দরকার। এখানে ঘটনার সাথে সংশ্লিষ্ট প্রতিটি আইটেম বা বিষয়কে বিবেচনায় এনে তাদের তথ্য পুঞ্জানুপুঞ্জ বিশ্লেষণ করা হয়। সেজন্য ইন্সিডেন্টে বিশ্লেষণের প্রতিটি পর্যায়ের প্রমানের ধারাবাহিকতা (Chain of Custody) রক্ষা করা হয়, যাতে ঘটনার পারস্পারিকতা সুস্পষ্টভাবে ফুটে ওঠে। ফলে ইন্সিডেন্টের আইনি গুরুত্ব ও গ্রহণযোগ্যতা (Legal Importance) বেড়ে যায়।

ইন্সিডেন্ট ব্যবস্থাপনার পর্যায়সমূহ (Steps of Incident Management)

ইন্সিডেন্ট লগিং
ফোন কল/এসএমএস/ইমেইল/লাইভ চ্যাট

ইন্সিডেন্ট লগিং
করাঃ প্রথমে
ইন্সিডেন্ট লগিং

করতে হবে। ইন্সিডেন্ট লগিং প্রক্রিয়া হতে পারে ফোন কল, ইমেইল, এসএমএস, সিস্টেম পর্যবেক্ষণ টুলের মাধ্যমে। ইন্সিডেন্ট লগিং এর মাধ্যমে এর পরবর্তী পর্যায়গুলোতে প্রবেশ করে এবং সংশ্লিষ্ট সবাইকে

ইমেইলের মাধ্যমে জানানো হয়। এর মাধ্যমে ইন্সিডেন্টের একটি একক নাম্বার দেওয়া হয়। এর ফলে অন্যান্য ইন্সিডেন্ট থেকে সহজে চিহ্নিত করা যায়।

ইন্সিডেন্ট শ্রেণী নির্ধারণ
উচ্চ / মধ্যম / নিম্ন

ইন্সিডেন্ট শ্রেণী
নির্ধারণঃ
ইন্সিডেন্টের

শ্রেণী/ধরন সাধারনত এটি কোন জাতীয় ইন্সিডেন্ট, কোন ভাইরাস/ ম্যালওয়্যার আক্রমন, অভ্যন্তরীণ ইনফ্রাস্ট্রাকচার কোন ব্যত্যয় এবং তার গুরুত্বের উপর নির্ধারণ করা হয়।

ইন্সিডেন্ট অগ্রাধিকার
গুরুতর / উচ্চতর / মধ্যম / নিম্ন

ইন্সিডেন্টের
অগ্রাধিকার
নির্ধারণঃ

ইন্সিডেন্টের গুরুত্ব, এর ক্ষতির মাত্রা ও এর জরুরীতার ভিত্তিতে অগ্রাধিকার নির্ধারণ করা হয়। অগ্রাধিকারগুলো সাধারনতঃ সঙ্কটাপন্ন/গুরুতর (Critical), উচ্চতর (High), মধ্যম (Medium) ও নিম্ন (Low) ধরনের হয়। এর ফলে প্রতিটি টিকেটে অগ্রাধিকারের ভিত্তিতে মনোনিবেশ দেওয়া হয়।

ইন্সিডেন্ট সমাধান

ইন্সিডেন্টের
সমাধানঃ এই
পর্যায়ে

ইন্সিডেন্টের মূল্যায়ন ও বিশ্লেষণ করা



হয়। বিভিন্ন তথ্য, উপাত্ত সংগ্রহ করে মূল কারন নির্ধারণ করা হয়। এরপর সমাধান করা হয়। এই পর্যায়ে সমাধানের প্রয়োজনে ইন্সিডেন্টকে উচ্চ পর্যায়েও পাঠানো হতে পারে অথবা সরবরাহকারীর (Vendor/Supplier) সাহায্যও নেওয়া হতে পারে।

ইন্সিডেন্ট সমাপ্তকরনঃ ইন্সিডেন্ট সমাধান করার পর এই সমাপনি পর্যায়ে যিনি ইন্সিডেন্টের মূল ভিক্টিম, তার মন্তব্য অত্যন্ত গুরুত্বপূর্ণ, তার সমস্যার সমাধান হল কিনা এবং ভিক্টিম সমাধানে সন্তুষ্ট হলে তিনিই ইন্সিডেন্ট সমাপ্ত করে দেন।



সাইবার ইন্সিডেন্ট ব্যবস্থাপনার সর্বোত্তম কৌশল (Best Practices for Cyber Incident Management)

ছোট, বড় যে কোন ধরনের প্রতিষ্ঠানের নিজস্ব সাইবার ইন্সিডেন্ট ব্যবস্থাপনার কৌশল থাকা প্রয়োজন। নিম্নে কিছু সর্বোত্তম

অনুশীলনগুলো(Best Practice) বর্ণিত হলঃ

- সিকিউরিটি ইন্সিডেন্ট ব্যবস্থাপনার পরিকল্পনা ও নীতিমালা (Policy) গঠন করা। যেখানে ইন্সিডেন্ট সনাক্ত করা, লগিং করা, মূল্যায়ন ও সমাধান করার বিস্তারিত নির্দেশিকা (Guidance) থাকবে। সাইবার শ্রেট অনুসারে কি পদক্ষেপ নেওয়া হবে, এই সম্পর্কিত একটা কার্যতালিকা (Checklist) থাকা বাঞ্ছনীয়, যা সময়ে সময়ে হালনাগাদ ও পূর্ববর্তী ইন্সিডেন্ট থেকে শিক্ষা নিয়ে নতুন ইন্সিডেন্ট সমাধানে প্রয়োগ করবে।
- ইন্সিডেন্ট প্রতিক্রিয়া টিম গঠন বাঞ্ছনীয়, যে টিমের সবার সুস্পষ্ট দায়িত্ব কর্তব্য বর্ণিত থাকবে। এই টিমে আইটি/সিকিউরিটি টিমের কার্যকর ভূমিকা থাকবে এবং অন্যান্য বিভাগ যেমনঃ লিগ্যাল, গণযোগাযোগ, অর্থ বিভাগ, ব্যবসায় ব্যবস্থাপনা ও পরিচালনা বিভাগ থেকে প্রতিনিধি থাকবে।

ইন্সিডেন্ট সমাপ্তকরন

- সিকিউরিটি ইন্সিডেন্ট ব্যবস্থাপনার কৌশলের উপর বিশদ প্রশিক্ষণের ব্যবস্থা থাকবে, এবং সাইবার সিকিউরিটির ভিন্ন ভিন্ন দৃশ্যপটের ভিত্তিতে কিভাবে মোকাবেলা করতে হবে, তার বাস্তব অনুশীলন থাকতে হবে।
- প্রতিটি সিকিউরিটি ইন্সিডেন্ট থেকে উত্তরনের পর তা থেকে শিক্ষণীয় বিষয়গুলোর আলোকপাত করতে হবে এবং কোন সমস্যা পাওয়া গেলে সেগুলো সারানোর উপর গুরুত্ব দিতে হবে।
- প্রতিটি সিকিউরিটি ইন্সিডেন্ট হ্যান্ডেল করতে পর্যাপ্ত, সঠিক ও যথাযথ (Sufficient, Right & Appropriate) প্রমান সংগ্রহের উপর গুরুত্ব দিতে হবে। সংগৃহীত প্রমাণসমূহ যথাযথ মানদণ্ড অনুযায়ী সংরক্ষণ করতে হবে। সেখেন্ত্রেঃ
 - যথাযথ প্রমান সংগ্রহের জন্য নীতিমালা থাকা বাঞ্ছনীয়, বিশেষভাবে কখন প্রমান সংগ্রহ করতে হবে এবং তা আদালতে উপস্থাপন করতে হবে।

- সংগৃহীত প্রমাণাদি কিভাবে নথিভুক্ত, বিশ্লেষণ ও তদন্ত করতে হবে তার বিবরণ।
- টিমের ফরেনসিক বিষয়ে প্রশিক্ষণপ্রাপ্ত ও যথাযথ বিভাগীয় জ্ঞানসম্পন্ন সদস্যদের কাজে লাগাতে হবে।

উপসংহার

সাইবার সিকিউরিটি ইন্সিডেন্ট ব্যবস্থাপনা অতীব গুরুত্বপূর্ণ এবং এর মাধ্যমে প্রতিষ্ঠানের সাইবার রিস্ক অনেক কমিয়ে আনা সম্ভব এবং পরিচালনা ব্যয়ের হ্রাসের মাধ্যমে গতিশীল ও নিরাপদ সাইবার ইনফ্রাস্ট্রাকচার গড়ে তোলা সম্ভব। এর জন্য পর্যাপ্ত জ্ঞান, সঠিক টুল নির্বাচন, এর যথাযথ প্রয়োগ, বাস্তব অনুশীলন জরুরী।

সূত্রঃ

- <https://digitalguardian.com/>
- <https://www.ncsc.gov.uk/>
- <https://www.manageengine.com/>



A Comparison of Global Data Localisation Policies and Frameworks

Pradeepta Sarkar

Education and Qualifications:

- Barrister at Law, Member of Lincoln's Inn
- CS50 for Lawyers under Harvard University
- Post Graduate Cyber Security Course from Amity Future Academy
- BPTC from City University of London (2018 - 2019) LLB Honours from Queen Mary University of London (2015 - 2018).

Introduction

Data localisation laws are legal measures designed to control/limit the *storage, processing* and *cross – border transfer* of domestic data to a specific geographical region or jurisdiction. These laws apply to entities that own or possess data (i.e. 'data controllers') and are usually implemented so that the country can control its domestic data access and usage.

Put simply they do two things:

- Requires data controllers to store and process data within the territory of the country
- Prevents or limits the transfer of domestic data out of the country's territory

The implementations of data

localisation laws are widely varied. Laws can be very stringent or relaxed; they can cover all types of data or very specific data sets. Different countries around the world have implemented such data localisation requirements in different formats. Without details as to what type of restrictions or policies the drafters want to follow, it is best to have a template from other countries to make such decisions. To that end, this paper is divided in to four more sections. Section 2 will look at the pros and cons of data localisation laws and provide examples of the various ways data localisation laws can be implemented. Section 3 will look the



data localisation laws of five different countries in detail. Section 4 will provide some analysis based on global trends that may be useful when



Pros and Cons of Data Localisation

Arguments for Data Localisation include:

- Information security – Global increase in cyber attacks post Covid 19 and data compromises make it sensible to place additional security measures on important data. A report by IBM on the cost of such breaches shows the impact globally is up to 4 million dollars. Different sectors that store and process data are affected differently, with Healthcare being the priciest industry for security incidents (\$429/record), followed by the Financial (\$210/record) and the Technology sectors (\$183/record). These costs might also explain the rationale behind some countries' decisions to focus on these sectors in their data localisation laws.²



Figure 3: Data Localisation Laws in ASEAN countries¹

² Cost of a data breach report, IBM, 2019

and create job opportunities. It also provides an advantage to domestic companies who will have an easier time complying than foreign companies trying to enter the market. However, data localisation might have an adverse impact since multinational companies might find it increasingly difficult to operate in multiple jurisdictions with different data localisation laws, leading to either an increase in cost of doing business in some countries or less incentive to enter such markets altogether.

- National data sovereignty and Law enforcement – Besides protecting data from foreign surveillance, data localisation serves the goal of making data available for the needs of domestic law enforcement. Since enforcement jurisdiction is primarily territorial, the location of assets or equipment in the jurisdiction may be justified as a way to make it easier to enforce local law.

Arguments against data localisation:

These are mostly economic or market driven. It is a simple fact that international trade involving consumers cannot take place without collecting and sending personal data across borders—such as names, addresses,

billing information, etc. Opponents to data localisation laws provide the following rationales:

- Discourages foreign investment - By impeding the free flow of data across borders, which is a basic requirement for businesses to digitize and stay competitive; and by running counter to international trade trends, MNCs are discouraged as they might find such regulatory ecosystems an unsafe place to invest. It makes the country's market seem less attractive.
- Creates more cyber security risks - Unlike data storage on international cloud servers, where if one network is down or compromised another network can be used to take its place, breach of a single local network can compromise the data of the entire country and effectively halt the flow of data. It is also said that data localisation laws force businesses to invest more on legal compliance measures, rather than actual cyber security tools.
- Lowers GDP - If data were restricted to remain in one country, multiple data centers would be required in the same country. Increased costs of storage would likely be passed



along to the consumer. Countries that enact barriers to data flows make it harder and more expensive for their businesses to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative goods and services that rely on data. The impact of such measures directly falls on the GDP. Figure 2 below provides an example of the impact of data localisation measures on the GDP and investment in member countries of ASEAN.

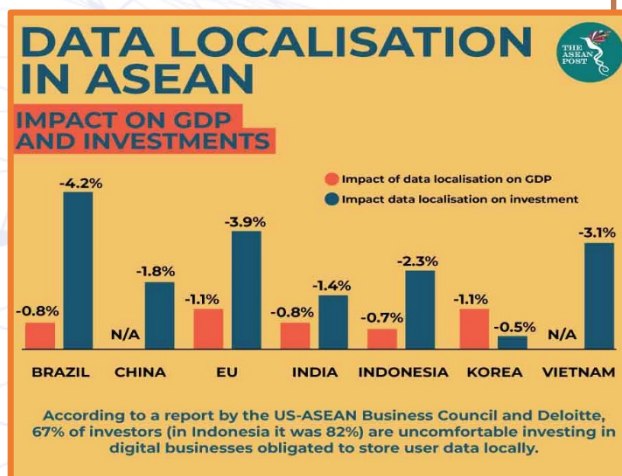


Figure 4: Impact of Data Localisation in ASEAN

Strictness of approach to Data Localisation

Despite having the common objective of keeping data within a jurisdiction, the degree of intrusiveness of data localisation measures varies from country to country. A number of regulatory tools can be used to implement localisation measures and they can be hard or softer alternatives.

The more categories or types of data that need to be localized, the more restrictive the measure becomes. Various tiers of measures exist and a group named 'deltapartners' have categorised them as follows³ based on their level of intrusiveness:

Data Sovereignty – All industries: Countries in this case require that all data related to their citizens be stored in servers physically located inside the country.

Data Sovereignty – Select industries: In this case, some data can leave country borders except for data related to some industries (the main ones being Financial services, Healthcare, Telecommunications and Government/Defense).

³ Mayssa, Keshav, 'Data localisation: From information protection to balkanisation of the Internet' (February 2020) <https://www.deltapartnersgroup.com/data-localisation-information-protection-balkanisation-internet>



In 2018, the Reserve Bank of India mandated that all payment system providers store payment data in the country, with similar measures planned for E-commerce, Social Media, Telecom and Healthcare. The UAE and Australia have similar measures for Healthcare data while Turkey imposes data localisation for Financial services.

Data Mirroring: This model allows data to cross country borders if a copy is stored locally. The revised Indian Personal Data Protection Bill, akin to the European Union's GDPR requires tech firms to have consumers' consent before collecting and processing their data. The data-mirroring requirement of this law requires that a copy of data on Indian citizens be stored in India. Similarly, the new Cybersecurity law of 2019 in Vietnam requires online service providers to store citizens' personal data inside the country.

Controlled localisation regulations: Less extreme laws that focus more on data privacy but have the side effect of indirectly encouraging data localisation.

Figure. 3 below produced by 'deltapartners' conveniently displays this broad spectrum of localization

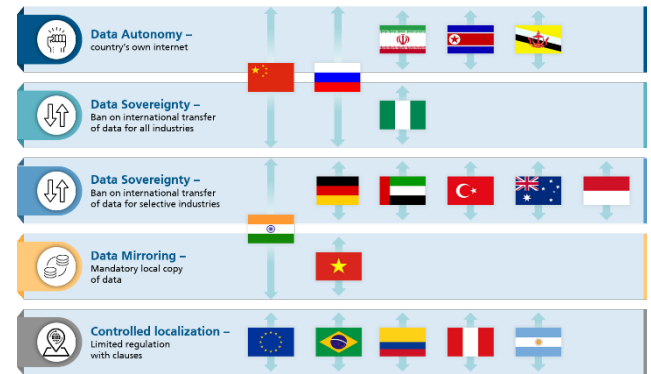


Figure 5: Different levels of Data Localisation across various countries

Explicit and Implicit Measures

Data Localisation Measures can also be further divided in to explicit and implicit types. 'Explicit measures' are hard measures that are very restrictive and directly enforce data localisation openly. They require, for instance, that the data be located on home country servers or that data processing is carried out within the national territory. They directly limit the storage, processing and transfer of data within a territory. On the other hand 'Implicit measures' indirectly enforce localisation in subtle ways. Examples of such measures would be how the EU or Australia does not allow the transfer of personal data outside their territories unless the recipient country has data protection measures and has been whitelisted. Various examples of explicit data localisation laws and implicit localisation laws are provided in the following chart.⁴

⁴ Handbook on Data Science and Law Chapter: Data localisation measures and their impacts on data science



| <i>Localisation measures</i> | | |
|---|--|--|
| Type of measure | Description | Example |
| <i>Explicit</i> | | |
| Local storage requirement | Requirement that data be stored on a local server. If it is stored in the cloud, it should be a local cloud. However, a copy of this data may be processed outside the national territory as well. | In Sweden, documents such as a company's annual reports, balance sheets and annual financial reports must be physically stored locally for a period of seven years; in Poland, any entity organizing gambling activities is obliged to store real time data exchanged between that entity and its users on a storage device located in Poland; ¹² in Russia, the law on data protection requires that personal data be stored domestically. ¹³ |
| Local processing requirement | Data must be processed within territory under a specified national jurisdiction. Processing has a broad meaning in data protection terminology and covers a wide range of activities, including storage, reuse and deletion. As 'processing' is a broader term than storing, a requirement to ensure local processing will typically be more restrictive than the requirement to store data locally. | In Luxembourg, financial institutions are required to process their data within the country. Processing abroad is permitted as an exception for an entity which is a part of the group to which the institution belongs or with its explicit consent. ¹⁴ In Turkey, companies that provide e-payment services are required to process data only within the national borders. ¹⁵ |
| Restrictions on data transfer | Data transfers are allowed only if the country where the recipients are located guarantees the same level of data protection as the country from which the data is transferred. | In the EU, personal data transfers to countries that do not ensure adequate levels of data protection are in principle prohibited. Exceptions allowing such transfers are permitted only under certain limited conditions. ¹⁶ |
| <i>Implicit</i> | | |
| Public procurement | Data flows are restricted through limits on procurement of foreign goods or services by governmental agencies, for example, requiring that information technology and communications services be obtained exclusively from local providers. | In Brazil, a presidential decree requires that federal agencies procure e-mail, file sharing, teleconferencing, and VoIP services from Brazilian 'federal public entities' such as SERPRO, Brazil's Federal Data Processing Agency. ¹⁷ |
| Requirements regarding local ownership/establishment/employment | Data flows are restricted by requiring that service providers have or establish in-country subsidiaries, branch offices or representation. These measures influence data flows by limiting foreign ownership and/or requiring joint ventures. ¹⁸ | In Kenya, the draft National Information and Communications Technology Policy encourages local employment in data centres. ¹⁹ |
| Other requirements regarding the use of local goods, services or content | Data flows are restricted by requiring use of locally provided services or locally generated content. They may also be limited to use of domestically made or locally sourced equipment; this entails a limited choice and perhaps impairs efficiency, but not data flows per se. ²⁰ | The German government has encouraged the construction of an EU Internet, and in 2013 Deutsche Telekom launched the E-Mail Made in Germany project that seeks to route data exclusively through domestic servers. ²¹ |
| Intellectual property (IP) export, import, and transfer control | Data flows are restricted by requiring corporate intellectual property and other technology to reside in-country. ²² | Although localisation measures are typically statutory, by-laws and other internal mechanisms which would preclude the escape of IP could be an example of localisation in corporate relations. |
| Traffic routing | Data flows are restricted by requiring communication service providers to route Internet traffic in a specific way. | India's former Deputy National Security Advisor, Nehchal Sandhu, reportedly sought ways to route domestic Internet traffic via servers within the country. ²³ While the effect of this rule would be the same as the effect of the requirement for local processing and/or storing of data, it focuses solely on directing data traffic. |
| Online censorship | Restricts data flows by blocking or filtering information transferred into or out of a country. ²⁴ | China and its Great Firewall is an example of modern internet censorship. The country has also taken a further step by barring foreign companies or their affiliates from engaging in publishing online content without government approval. ²⁵ |



Global data localisation laws

Section 2 has hopefully provided a good idea of why data localisation takes place and how it can be implemented in different ways depending on the objective of the legislating country. This section is intended to provide a more in-depth look at the data localisation laws of 5 select countries which employ a wide range of data localisation laws, ranging from various explicit measures resulting in complete data sovereignty to less intrusive data localisation laws. The hope is that they form a good basis for drafting similar laws for Bangladesh. These countries are as follows:

- 1) Russia
- 2) Vietnam
- 3) China
- 4) India
- 5) Turkey

Russia



Types of Data Localised: Personal Data and Telecommunications Data

Russia operates one of the most extensive sets of data-localization policies in the world. In 2015, Russia enacted a Personal Data Law. Article 8 of the Act mandates that data operators who collect personal data about Russian citizens must “record, systematize, accumulate, store, amend, update and retrieve” data using databases physically located in Russia⁵. This personal data may be transferred out, but only after it is first stored in Russia. The declared goal of this data localisation measure is to end uncontrollable use of data in foreign states and improve protection of the personal data of Russian citizens. ⁶Russia has threatened to shut down and fine websites, such as LinkedIn, that refuse to store data locally.

Failure to comply with the data protection requirement may lead to blocking the website used to process the data. This was the case for LinkedIn. LinkedIn failed to provide

⁵ 9 Federal Law of the Russian Federation No. 152-FZ] (n 14).
<https://platform.dataguidance.com/legal-research/federal-law-21-july-2014-no-242-fz-amending-some-legislative-acts-russian-federation>

⁶ ‘Основные положения Федерального закона № 242-ФЗ’ (пд-инфо.рф) [‘Main Provisions of the Federal Law No. 242- FZ’] 2
http://pdinfo.ru/upload/docs/slides_242.pdf



Roskomnadzor with evidence that it stores the required data in Russia, and Roskomnadzor sued LinkedIn in a Russian court. The court ruled against LinkedIn and ordered

Roskomnadzor to block access to LinkedIn.¹⁰⁸ Following an unsuccessful appeal, Russian Internet access provider's restricted access to LinkedIn.⁷ Russia also fined Facebook and Twitter up to 51,000 Euros for failing to meet localisation requirements in Decisions of the Magistrate Court of Judicial District No. 374 of Tagansky judicial district of Moscow of 13 February 2020 Cases No 5-167/2020 here).

Furthermore, in 2016, Russia enacted extensive new data-localization requirements for telecommunications data under the Yarovaya Law. Russia's approach is much broader than other countries' telecommunications data-retention requirements, as it requires companies to store the actual content of users' communications for six months, such as voice data, text messages, pictures, sounds, and video, not just the metadata (the who, when,

and how long of communications). Second, it requires telecommunications companies and ISPs to cut services to users if they fail to respond to a request from law enforcement to confirm their identity. Telecommunication operators are now obliged to retain not only metadata and some types of personal data of users (as prescribed by the Data Localisation Law), but also to retain the content of users' communications and enable Russian security authorities to decrypt messages if the moderator applied encryption (cryptographic) tools. Failure to comply with the said obligations may result in a fine of up to RUB 1 million (approx.

€12,900).

The Act also applies similar requirements on 'so – called 'moderators of dissemination of information on the Internet. The statutory definition of moderators is indeed quite broad. Moderators are defined as: "Entities maintaining information systems and/or software, which are designed and/or used for the receipt, transfer, delivery, and/or processing of messages on the internet." At first sight, such a notion applies mainly to instant messaging, blogging, social media, public e-mails, etc. However, the broad and

⁷ Москва. Суд. Апелляционное определение от 10 ноября 2016 года по делу № 33-38783/16 [Moscow Judicial System, Appeal Decision of the Moscow City Court in Case No. 33-38783/16 < <https://mosgorsud.ru/mgs/cases/docs/content/c364d1d9-e30c-4ffa-aabb-327c8977adab>>



ambiguous definition makes it possible to apply the law to every website containing a forum or the option of providing feedback for its users, as well as companies maintaining corporate communication systems.

Exceptions from data localisation are very limited and connected to data processing conducted by the state, in compliance with international agreements or national laws, or in connection with litigation and processing by journalists and media.

Vietnam



Types of Data Localised: Emerging Digital and Internet Services, Social Media and Telecommunications Data

Vietnam has extensive data-localization policies in place as part of broad efforts to control Internet-based activities (for both political and commercial purposes). For example:

- Vietnam forbids direct access to the Internet through foreign ISPs and requires domestic ISPs to store information transmitted on the Internet for at least 15 days.
- In January 2016, Vietnam released a draft regulation—Draft Decree Amending Decree 72—for over-the-top services (such as WhatsApp and Skype) that included a forced data-

localization requirement. The Draft Law expands data localization provisions to: Include “local and foreign agencies and entities, when providing services on cyberspace or owning any information systems in Vietnam,” in (Article 26.2.) Require corporations to “set up their mechanisms to authenticate information when users register digital accounts... [and] provide the users’ information to the specialized force in charge of cybersecurity protection... in writing,” in (Article 26.2(a)) Grant the Vietnamese government unrestricted power in the future to “detail what types of information shall be stored in Vietnam and which enterprises are required to locate their head offices or representative offices in Vietnam,” in (Article 26.3)

- In 2013, Vietnam enacted a law—Decree 72—on the management, provision, and use of Internet services and online information that requires a broad range of online companies (such as social networks, online game providers, and general information websites) to have at least one server in Vietnam “serving the inspection, storage, and provision of information at the request of competent state management agencies.”
- In 2008, Vietnam enacted a law—Decree 90—against spam (unwanted emails and text messages) that forces relevant advertising companies involved in these activities



to send emails and texts only from servers in Vietnam

More recently, On 23 April 2020, the Ministry of Information and Communications (MIC) released a Draft Decree, amending Decree No. 72/2013/ND-CP on the management, provision, and use of Internet services and online information and Decree No. 27/2018/ND-CP.

The Draft Decree⁸ contains certain notable changes to the regulations on online information and the use of Internet services, including:

(1) New categorization of online information: The Draft Decree lists out the following as forms of online information: Electronic newspapers; Aggregated news websites, Internal websites; Personal websites, as established by individuals or established using the social networking platforms to provide and exchange information of their own, Professional websites, as established by organizations, agencies, and enterprises providing services in the fields of telecommunications, IT, radio,

television, commerce, finance, banking, culture, healthcare, education and other professional fields; and Social networks, including multi-service social networks.

(2) New provisions on cross-border provision of public information and personal data: Articles 3.4 and 5.1 suggest that personal data may only be used with the consent of the data subject or permission of the competent authorities or as otherwise provided by law. However, Article 14 suggests that there may be some circumstances in which personal data may be processed without the consent of the data subject.

Article 66.4 states that it is the responsibility of owners of information systems critical to the national security “When collecting or creating personal information and critical data, to store the same within the country. Where it is obligatory to provide any information out of the country, to assess security levels as regulated by the Ministry of Public Security or in accordance with legislation where it provides for this.’

In addition, Vietnam requires that local and foreign enterprises, which provide

8

https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/vietnam-ministry-of-information-and-communications-release-new-draft-decree-amending-earlier-decrees-covering-the-management-provision-and-use-of-internet-services-and-online-information



services on telecom networks and on the internet and other value-added services in cyberspace in Vietnam, and which carry out the activities of collecting, exploiting, analysing and processing of data about personal information, data about service users' relationships and data generated by service users in Vietnam, must store such data in Vietnam for a specified period to be stipulated by the Government. In particular, these enterprises must have their branches or representative offices in Vietnam.

(2) New licensing requirements for establishing websites, aggregated news websites, social networks, application distribution stores and online games: Foreign public information providers that rent storage in Vietnam to provide services, or those with more than 1 million interactive users in Vietnam per month, are required to:

- Provide certain information to the MIC, such as registered name, address, nationality, contact details, locations of the main servers, etc.;

- Cooperate and take down information that violates Article 5.1⁹ of Decree No. 72; in particular, within 24 hours

Under the Draft Decree, social networks are now categorized into:

- a) Social networks with high levels of interaction (i.e., more than 1 million interactive users in Vietnam per month, or more than 10,000 registered users per month): these must register for a Social Network License;
- b) Social networks with low levels of interaction (i.e., less than 1 million interactive users in Vietnam per month): these must notify the MIC.

The MIC will embed a tool to monitor the interaction of users on social networks and will review if such social networks should apply for applicable licensing procedures. Only licensed social networks are allowed to charge users for service fees (in any form) and to provide live streaming services.

⁹ Article 5. Prohibited acts

1. Using the provision and use of internet services and online information for:

- a) Opposing the Socialist Republic of Vietnam; threatening the national security, social order and safety; sabotaging the national fraternity; propagating wars and terrorism; and arousing animosity among races and religions.
- b) Propagating and inciting violence, obscenity, pornography, crimes, social problems, superstition; contradicting national traditions;
- c) Revealing state secrets; military,

economic, and diplomatic secrets; and other secrets defined by the State;

d) Providing false information, slandering or damaging the reputation of organizations or the dignity of individuals; dd)

Advertising, propagating, trading in banned goods or services; spreading banned publications;

e) Impersonating other organizations and individuals to spread false information, which violates the lawful rights and interests of other organizations and individuals.



The Draft Decree also sets out new requirements for social networks to include the following:

- To have one person, who is a Vietnamese citizen and has experience in journalism management or has a university degree in journalism, in charge of content management;
- To have a mechanism for removing illegal content within three hours after self-discovery or upon request from the MIC;

Vietnam applies a mix of explicit and implicit measures to create a comprehensive data localisation schema under the guise of a cyber security act. Comments by several international bodies such as the 'Software Alliance', BSA and Asia Internet Coalition have pointed out these measures and have advised against their implementation, however the most recent update of the Decree seems to indicate that the recommendations were ignored.

China

Types of Data Localised: Accounting, Tax, and Financial, Personal, Emerging Digital Services, Social Media

China has one of the widest sets of data-localization policies, which stops the flow of data between China and the

rest of the world. To start with, it has long limited data "imports." For example, the Ministry of Public Security runs the Golden Shield program (commonly referred to as the "Great Firewall of China"), which restricts access to certain websites and services, particularly ones that are critical of the Chinese Communist Party. As the cross-border data transfer rules mainly aim to protect national security, they are far-reaching and leave regulatory authorities plenty of room for discretion. The majority of laws relate to foreign and domestic enterprises with business operations in China. Additionally, any organisation or individual would be subject to the law if they collect, process or use personal information of Chinese citizens within the territory of China, or if they transfer such data into or out of China. The law does not exempt any sector or institution from adherence to the requirements of due process in the performance of their respective offices, and no areas are beyond its scope.

From a trade perspective, China has made several policy changes in the wake of the Snowden revelations that restrict the cross-border transfer of data. For example:

- In 2006, China introduced measures for e-banking that require



such companies to keep their servers in China.

- In 2011, China introduced a law that prohibits the off-shore analyzing, processing, or storage of Chinese personal financial information.
- In 2013, China enacted new rules regarding credit reporting that requires all credit information on Chinese citizens to be processed and stored in China.
- In 2014, China enacted new rules that require health and medical information to be stored only in China.
- In 2015, China released draft administrative regulations for the insurance industry that included localization requirements.
- In 2016, China enacted new rules the forced companies involved in Internet- based mapping services to store data locally.
- In 2016, China issued new rules regarding online publishing that require all servers used for a broad range of services involved in online publishing in China to be located in China. This includes app stores, audio and video distribution platforms, online literature databases, and online gaming.

- In 2016, China's new Counter-Terrorism Law requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities. Any movement of data offshore must undergo a "security assessment."
- In 2016, China enacted a new cybersecurity law that forces a broad range of companies to store users' personal information and other important business data in China.
- In March 2016, China enacted new regulations regarding cloud-computing services in China that essentially exclude foreign technology firms and reinforce local data-storage requirements.
- In April 2017, China released a draft circular that outlined extensive localization requirements—both explicit and implicit—as part of a restrictive regime of "security checks" for businesses wanting to transfer data overseas, further to the cybersecurity law, which outlined the need for such security assessments. This draft extends data localization from "critical information infrastructure" to all "network operators," which is likely any owner or administrator of a



computerized information network system. Furthermore, any outbound data transfer would be prohibited if it brings risks to the security of the national political system, economy, science and technology or national defense.”

For future updates and for referencing purposes the bulk of China’s data localisation laws can be found in the following link (<https://www.dataguidance.com/opinion/china-data-localisation-requirements>)

A full translation of China’s Cyber Security Law as of 2017 can be found here:

<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/#:~:text=Article%2037%3A%20Critical%20information%20infrastructure,store%20it%20within%20mainland%20China.>

General data localisation requirements can be found in:

- Article 37 of the Cybersecurity Law of People's Republic of China ('CSL'), which requires critical information infrastructure operators ('CIIOs') to store

personal information and important data generated from critical information infrastructures in China;

- Draft Data Security Law of People's Republic of China ('the Draft Data Security Law'), which was reviewed by the National People's Congress of the People's Republic of China ('NPC');
- the Measures for the Assessment of Outbound Security of Personal information and Important Data (Draft for Comments) of 11 April 2017 ('the Old Measures'), which are not currently effective;
- the Measures for the Assessment of Outbound Security of Personal Information (Draft for Comments) of 13 June 2019 ('the New Measures'), which are also not currently in effect; and
- The Information Security Technology-Guidelines for Data Cross-Border Transfer Security Assessment (Draft for Comments) ('the Draft Guidelines') of 25 August 2017, also not effective.



Special data localisation provisions can be found in:

- Article 48 of the Law of the People's Republic of China on Guarding State Secrets (2010 Revision), which provides that if the data is related to state secret of China, such data is prohibited from being transferred outside to third countries and must then be stored exclusively in China;
- Article 6 of the Notice by the People's Bank of China Regarding the Effective Protection of Personal Financial Information by Banking Institutions provides that personal financial information collected in China shall be stored, processed, or analysed in China; except when otherwise required by other laws and regulation, banking financial institutions shall not transfer domestic personal financial information outbound China;
- Article 24 of the Regulation on the Administration of Credit Investigation Industry states that information collected by credit investigation organisations shall be stored in China; if such organisation needs to transfer personal information outbound China, it shall comply with the relevant requirements of laws and regulations;

- Article 10 of the Measures for the Administration of Population Health Information (for Trial Implementation) provides that population health information is prohibited from being stored in servers located outside of China;
- Article 27 of the Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions states the information of lenders and borrowers collected in China shall be stored in China; except when otherwise required by other laws and regulations, the online platform should not transfer the information of the lenders and borrowers outside of China;
- Article 34 of the Regulation for the Administration of the Map ('the Regulation for Map Administration') states that internet map service organisations shall set up a server for storing map data within the territory of the People's Republic of China, and build up an internet map data security management system and safeguards;
- Article 27 of the Interim Measures for the Administration of Online Taxi Booking Business Operations and Services provides that online taxi platform companies should comply with the relevant national



network and information security provisions; that is, the personal information and business data should be stored and used in mainland China, shall not be transferred outside of China, and should be retained for two years, except for when otherwise required by other laws and regulations; and

- Article 4 (13) of the Guiding Opinions of Encouraging and Regulating the Development of Internet Bicycle Rental provides that the server of internet bicycle rental operators shall be located in China, and the personal information and business data should be stored and used in mainland China.

In some instances, some categories of data can be transferred after localisation. Under Article 37 of the CSL, if it is indeed necessary to provide such information and data overseas due to business needs, a security assessment shall be conducted in accordance with the measures developed by the Cyberspace Administration of China in conjunction with the relevant departments of the State Council, unless it is otherwise prescribed by any law or administrative regulation. Under the CSL, the data can be transferred

outside of China if the result of the security assessment is positive.

Contrary to common belief, China does not require all network operators to comply with the data localisation provisions, and does not prohibit all data from being transferring outside of China. Currently, CIIOs in China must store their data in China, including personal data and important data generated from their important networks and systems. For most of organisations, which are not a CIIO, they may consider to a security assessment when the need arises to transfer data outside of China. Despite this China is definitely the country with the most expansive and explicit data localisation acts in history.

India



Types of Data Localised: Accounting, Tax, and Financial, Government and Public

Compared to the previous countries, India has far less strict regulations requiring data localization. India's Ministry of Communications and Technology enacted data transfer requirements as part of a 2011 change to privacy rules that could be used to



restrict data flows containing personal information. These rules limit the transfer of “sensitive personal data or information” abroad to only two restrictive cases—when “necessary” or when the subject consents to the transfer abroad. Because it is difficult to establish that a transfer data abroad is “necessary,” this provision would effectively ban transfers abroad except when an individual consents. The ministry clarified that these rules only apply to companies gathering data on Indians and only when the company is located in India. On paper these laws are restrictive, however, India has thus far not used the law to require local data storage. Other notable localisation requirements are listed below:

In 2012, India enacted a “National Data Sharing and Accessibility Policy,”¹⁰ which effectively means that government data (data that is owned by government agencies and/or collected using public funds) must be stored in local data centers.

In February 2014, the Indian National Security Council proposed a policy that

would institute data localization by requiring all email providers to set up local servers for their India operations and mandating that all data related to communication between two users in India should remain within the country.

In 2014, India’s enacted the Companies (Accounts) Rules law¹¹ that required backups of financial information, if primarily stored overseas, to be stored in India.

In 2015, India released a National Telecom Machine-to-Machine roadmap that requires all relevant gateways and application servers that serve customers in India to be located in India. The Roadmap has not yet been implemented. Indian government agencies have also made data localization a requirement for cloud providers computing for public contracts. For example, in 2015, India’s Department of Electronics and Information Technology issued guidelines that cloud providers seeking accreditation for government contracts would have to require them to store all data in India.

¹⁰ http://164.100.47.193/Refinput/New_Reference_Notes/English/Digital_India.pdf

¹¹ <https://taxguru.in/company-law/companies-act-2013-companies-accounts-rules-2014.html>



Turkey

Types of Data Localised: Personal, Accounting, Tax and Financial

Turkey has extensive data localisation regulations. The notable ones are as follows:

Recently in 2019, The Information Technologies and Communication Authority in Turkey published two decisions regulating embedded SIM technologies, requiring localisation for e-call systems. This has caused much controversy, as it strictly requires localization of data storage and eSIMs to be used in the devices regardless of the aim and type of communication activity for all devices that use eSIM technology. The regulation set a deadline for operators to comply with the localization requirements. The BTK has reserved the right to deactivate all devices operating within Turkish borders that fail to comply with the decision. The impacts on the automotive industry and the electronic communication industry, of such localisation requirements have been dire, especially for foreign firms.

In 2013, Turkey enacted a law—the Law on Payments and Security Settlement Systems¹², Payment Services and Electronic Money Institutions—that forces Internet-based payment services, such as PayPal, to store all data in Turkey for ten years.

"Keeping records and documents, protection of personal information, notification of changes ARTICLE 23- (As amended by Law No. 6637 of March 27, 2015) (1) The system operator, payment institution and electronic money institution shall be required to keep all the documents and records related to the matters within the scope of this Law for at least ten years in the country, in a secure and accessible manner..."

PayPal withdrew from the country after refusing to abide by this data localization requirement.

In 2016, Turkey enacted the Law on the Protection of Personal Data, which limits transfer of personal data out of Turkey and may require firms to store data on Turkish citizens in country. The law places burdensome obligations on

¹² <https://www.kilinlaw.com.tr/en/electronic-money-and-payment-institutions-in-turkish-law/>



data controllers and processors, requiring “express consent” from individuals to transfer personal data to another country. The need for specific and individual engagement holds the potential to act as de facto data localization. Turkey’s new law adopts a similarly untenable and unrealistic approach to international data flows and protection as that of the European Union by requiring country- by-country assessments of privacy protections. Under this law, if the country receiving data from Turkey does not offer “adequate” protection, the Data Protection Board must provide permission for each transfer.

Summary Analysis

The five countries and their localisation laws outlined in Section 3 above provide a sample of different localisation regulations and most of the acts can be accessed via links in the footnotes. A larger data sample can be obtained from the following site:

<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

For easy reference, a quick summary of which jurisdictions have localisation laws for the main types of data sets is as follows:

- Overarching personal data regime: Argentina, Australia, Brazil (upcoming), Chile, Colombia, Egypt, European Union, Ghana, India (upcoming), Indonesia (upcoming), Japan, Lesotho, Mexico, Peru, Singapore, South Africa, South Korea and Uruguay.
- o Banking/finance specific: Australia, Chile, China, Colombia, European Union, Ghana and Singapore;
- o Cybercrime / cybersecurity specific: China and Egypt;
- o Healthcare specific: Australia, China and the European Union; and
- o Telecommunications specific: Argentina, Australia, China, Egypt, European Union, Ghana, India and Singapore.



Important Observations for Bangladesh

- 1) GATS/WTO Membership - Bangladesh is a member of the WTO and GATS and has made commitments in pursuance of free trade agreements. Introduction of data localisation laws may be against such commitments. The GATS applies to measures affecting trade in services, covering four possible modes of trade in services across borders. Under the GATS, WTO Members are subject to various obligations to liberalize trade in services. Some GATS obligations are of general application, applying to all WTO Members and all service sectors. Other obligations are specific, and function on the basis of commitments that WTO

Members have made in respect of specific service sectors. WTO Members may lay down commitments to permit access to foreign services and service suppliers into their markets (market access commitments) under Article XVI, and commitments to treat foreign services and service

suppliers no less favourably than their domestic counterparts (national treatment commitments) under Article XVII. GATS market access obligations may apply to data localization requirements, because such requirements may serve as barriers to the cross-border provision of services by Foreign Service suppliers.

While the GATS can work to discipline data localization requirements, it has certain limits in this regard. It does not contain provisions dealing explicitly with data localization, nor is there WTO jurisprudence expressly considering data localization. There can be diverse range of objectives underlying data localization requirements, including 'privacy, cyber security, national security, public order, law enforcement, taxation, and industrial development, among others'. Under the GATS, countries are permitted to derogate from their trade liberalization commitments on the basis of specified countervailing public policy objectives. Data localization requirements may be exempted under Article XIV, which exempts measures necessary to



maintain public order and to secure compliance with laws or regulations, among other things. Article XIV can also exempt data localization measures as measures necessary to protect national security interests. Care should be taken therefore, to have justifiable reasons for any data localisation laws.

- 2) Lengthy adoption time – When localisation laws were introduced in Vietnam, the MPS expected domestic businesses to comply with the data localization and local office requirements within 1 year. However this was too short and a period of at least 3 years was recommended upon review of the law. It needs to be borne in mind that facilitating local storage of data is a expensive, costly and time consuming venture. Adoptions of local data storage requirements are bound to take some time especially for Bangladesh which does not have any previous data localisation measures.

- 3) Possible impact on FDI and GDP – As noted previously, explicit data localisation requirements would stand to discourage foreign

companies from entering local markets and this may impact foreign investment and economical growth. Membership to ASEAN in the future may also result in relaxation of any laws implemented at this stage. Data localisation laws should be limited to specific sectors or types of data such as medical or telecommunications data to lessen any negative impacts. This is because a blanked localisation requirement is difficult to implement, enforce and sustain.

Conclusion

The aim of this paper has been to provide a comparison between the data localisation laws of different countries and analyse such laws in some detail to assist in the drafting of such laws. Despite diverging world views, it is undoubted that data localisation and how widely its adopted will greatly shape the digital economy of the future.



Traditional VAPT VS Effective Security Assessment Program For Enterprises

Mohammad Makchudul Alam, Incident Handler

Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

"Cybersecurity Professionals Need To Win Every Time, But An Attacker Only Need To Win Once!!!"

Now a days VAPT becomes more essential tasks required for the organizations to keep their Cyber/ IT enabled Information Systems secure against the ongoing cyber threats. Performing VAPT is also treated as mandatory requirement by some compliances like as PCI-DSS.

Gaps in traditional VAPT

"Cost of a Data Breach Always Much Higher Than Cost Of Effective Security Testing!"

- In most cases VAPT is driven by the compliance and regulatory requirements rather than focusing (ensure/ enhancing) the security and safety of the organization's cyber space.
- Till now in our country, most organization don't have independent information security dept. or team, whereas security team is formed within IT dept. and due to lack of

effective Information Security governance and conflict of interest, IT Security team can't enforce other adjacent teams regarding the detected/ unpatched vulnerabilities.

- As always business dominates the organization, by nature business team always try to deny the update/ change due to any vulnerability by showing business losses (whereas they even don't have interest to realize the aftermath of an incident due to such vulnerabilities.)
- In some organization, VAPT within a network exercise only focused to the servers, hosts or endpoint devices where they ignore network devices (Router, Switches, Firewalls etc.) from the scope, which also may vulnerable and crucial to make the perimeter secure.
- Unfortunately, without realizing the cost of a breach, Pentest/ Red team assessment assumes costly in our industry.
- Proper knowledge regarding the red team/ pen-test engagement processes, tools, techniques, exploitation as-well-as the purpose and expected outcome from such security testing.
- In some cases, 3rd party vendors or service providers may have intention to reduce the workforce to discover and exploit vulnerability with deep-drive, due to feasibilities of timeframe, unskilled resources or any other issues.
- Finally, shortage of experts in our industry.



Why need effective exploitation of vulnerabilities through security testing?

"Continuous Patching & Updating/ Upgrading The Systems Or Assets In Timely Fashion Is Really A Boring Tasks, And We Always Love To Lead A Hassle-Free Work."

Though everyone knows that vulnerable service or products are needed to avoid and replace/ update by considering the organization's safety, but end of the day some people also thinks that hackers can't find their vulnerabilities and they are not in such danger. This is also considerable that, system/ asset owners are always passing busy time to keep the service up with no interruption.

"100% Service Uptime Without Secure Measures Lead to Such Situations"



Fig: [Ref: <https://www.mediagistic.com/blog/the-leaky-bucket-syndrome-are-you-set-up-to-handle-inbound-web-leads>]

So, effective security testing and assessments may helpful:

- To draw a clear picture of remaining vulnerabilities and risk factors to the organization's assets.
- To defend against our demotivation of keeping the systems up-to-date, successful exploitation of vulnerabilities to show the level of security posture through effective security testing and assessment is necessary.
- Such exploitation may effective to make conscious all of stakeholders to keep their systems/ assets up-to-date from the released vulnerabilities.
- To ensures whether suitable security policies are being followed or not

Effective security assessment and vulnerability management program

This is recommended to initiate and maintain an organization wide security testing and vulnerability management program to better adherence of the security culture among the all entities to the organization. An effective vulnerability management program may include:

- Define the Testing scopes and assessment criteria along with definition of terms and conditions.
- Security Testing of all the assets and applications.
- Remediate and resolve the detected vulnerabilities.



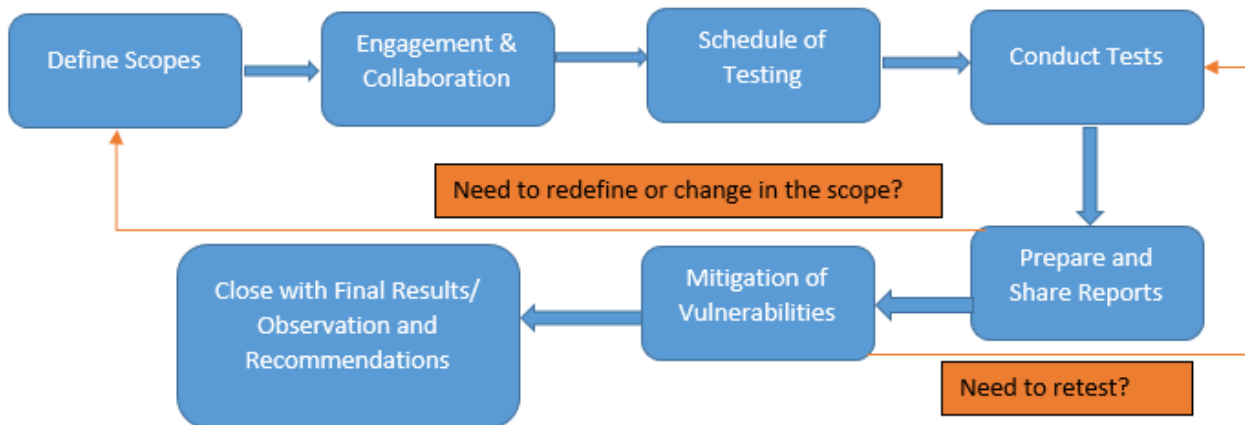


Fig: Typical Security Testing workflow

- Final Report submission along with observation and recommendations.

Scoping for the security testing

- Define the scope of pen-test or Red Team wisely and consider to coverage of most of the assets within the whole network (without considering only PCI DSS, SWIFT or ISO zones or networks), as we should consider that security is required for organization's safety not only for compliance.
- Don't rigid the scope within defined lists of assets, also encourage teams to discover and test the hidden or chain vulnerable assets (discovered during the pen-test) and adjust these in final VAPT scope.
- Include fire-walking, network segmentation test and FW Ruleset review to check the effectiveness of Firewalls and zone configurations. Also include network devices in VAPT

checklists to identify and patch-up vulnerabilities in timely manner.

- Regularly test the web based and other application in regards to OWASP top 10 and other well-known application and API related vulnerabilities (APIs are currently focused as one of the top attack vectors).
- Always think twice before finally declare the scope of assessment and rule of engagements.
- Some considerable tasks may define in scope of security testing:
 - Vulnerability Scanning & Penetration Testing of all Servers, Network Devices and Databases
 - Testing of all Application Servers resided in the DMZ, DNS, Proxy servers.
 - Testing of web applications including all e-commerce portals, PG and all other public facing systems.
 - Fire-walking, Firewall rulesets review, Network Segmentation Tests



- Rogue wireless AP detection tests (Wireless scanning)
- Check for unauthorized physical access control within the secure areas
- And many more!!!

Scheduling of assessments/ tests

To get effective outcome from security assessment and testing this is recommended to prepare a plan and feasible schedule by considering the

testing is performed and vulnerabilities are mitigated.

- To trace Gaps in testing scopes
- To meet the compliance requirements as-well-as keep the systems up-to-date from ongoing vulnerabilities
- To define annual forecast as tasks for the security testing teams

A typical schedule for the tasks associated with security testing and assessments is defined here, which illustrates how an Information Security Team can define the network segments

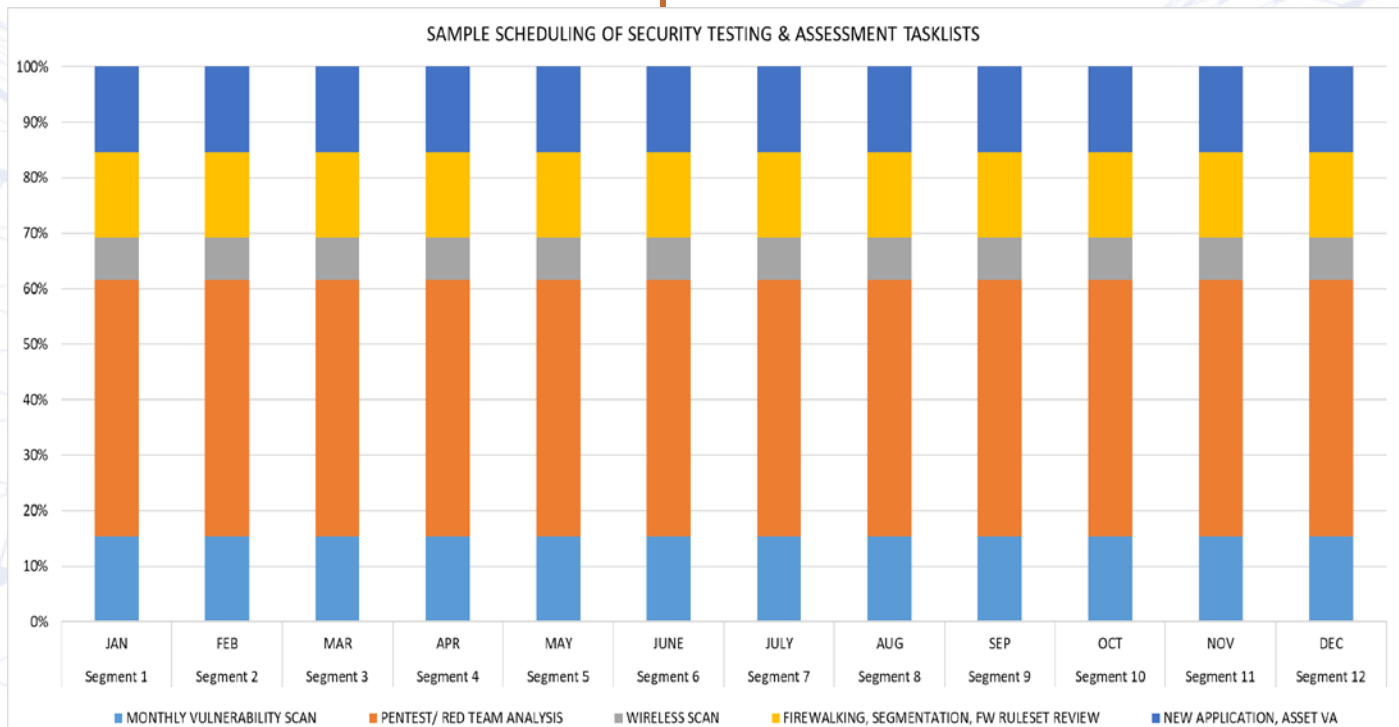


Fig: Sample Projection of Yearly Security Testing and Assessments

scope and timeframe. An appropriate testing schedule may help organizations:

- To keep proper track of the assets and or applications, to which

and other applications as-well-as tasks for Pen-Testing/ Red Team Assessments.



Considerable Assessment Feasibility

- Security tester should be free to discover residing vulnerabilities by considering the avoiding of interruption of services.
- If any test has possibilities to disrupt the services, then security tester should inform relevant administrator or entity regarding the test and choose a suitable time to perform such tests.

detected vulnerabilities by the automated vulnerability scanner).

- Security tester or 3rd party service provider must conduct a NDA along with rules of engagements regarding the disclosure of detected and exploited vulnerabilities prior to perform any security testing.
- Security tester may have freedom to choose tools and techniques preferred by them, but to conduct vulnerability scan for any specific compliance they should use

| SECURITY TEAM ANNUAL TASK LIST | | | | | | | | | | | | | | |
|---|---|---|---|-----------|-----------|--|-----------|-----------|--|-----------|-----------|--|------------|------------|
| AGENDA | TASK LISTS | Functional Activities | JAN | FEB | MAR | APR | MAY | JUNE | JULY | AUG | SEP | OCT | NOV | DEC |
| Cyber Security Assessment, Testing and Validation | Regular Assessment/ Testing Scope | Smaller Segments including Application and All Services including : > All Servers, Network Devices, DBs > Public Facing Systems, Web Applications etc. | Segment 1 | Segment 2 | Segment 3 | Segment 4 | Segment 5 | Segment 6 | Segment 7 | Segment 8 | Segment 9 | Segment 10 | Segment 11 | Segment 12 |
| | SEGMENTATION TEST FOR COMPLIANCE VALIDATION | Perimeter Testing for Compliance Validation > Tests to ensure all Firewall rules between 2 network segments are in track | Network Specified in PCI Scope | | | Network Specified in ISO Scope | | | Network Specified in Other Scope | | | Network Specified in Other Scope | | |
| | WIRELESS SCAN | | 25th of each month | | | | | | | | | | | |
| | ASV Vulnerability Scan | | Monthly vulnerability Scan program for all defined scopes (different services, applications, new project etc.) | | | | | | | | | | | |
| | PERIODIC PENTEST | > Active and Passive Phishing > Identify issues in source code of internal products or services > Can be done for external code bases > Test all built exploits in a Development environment | Regular Pentest Program for all organizational scopes (different services, applications, excluded in PCI scope, new project etc.) | | | | | | | | | | | |
| | PROCESS MANAGEMENT CHECK | | Check for common hardening and Patching status | | | Check for common hardening and Patching status | | | Check for common hardening and Patching status | | | Check for common hardening and Patching status | | |
| | FW Ruleset Review | | FW 1 | | | FW 2 | | | FW 3 | | | FW 4 | | |
| | AWARENESS TRAINING | | Quarter- 1 | | | Quarter- 2 | | | Quarter- 3 | | | Quarter- 4 | | |

Fig: Sample Annual Security Assessment and Testing Related Task Lists Scheduling

- Tester should follow the declared timeline to test the specific assets or application as prescheduled manner.
- Security tester should have encouraged to discover the hidden vulnerabilities or 0-days by assessing the codes or asset configurations with deep-drive (not only look for the

compliance validated scanner (like as for PCI DSS compliance this is mandatory to use any ASV scanner for vulnerability scanning.)

Qualities for a qualified Security Assessor/ Tester:

- Clearly understand the scope of work, assets within the scope, restrictions, allowed methods, tools or techniques.



- Critical and off-the-box thinking and hacker approach
- Choose a suitable set of tests as well as tools that balance cost and benefits
- Follow suitable procedures, standards and techniques with proper planning, documentation and evidences (PoCs).
- Establish the scope for each penetration tests, such as objective, limitations and justification of procedures.
- Be ready to show how to exploit the vulnerabilities also regeneration of exploitation if needed.
- State the potential risks along with risk ranking, possible threat sources and other findings in the report.

Remediation of Vulnerabilities

Though, this is recommended to remediate all the detected vulnerabilities within shortest period of detection, but in practical some vulnerabilities are not possible to patch-up ASAP due to dependency of release patches from the vendors or any other dependencies. In such scenarios:

- Administrators or asset/application owner should prepare a detail plan for the feasible remediation of vulnerabilities.
- Deploy the compensating control to uncovered vulnerabilities
- Should prepare a risk acceptance by defining/ demonstrating the proper difficulties, reasoning and dependencies.



- Provide suggestions and references for feasible and possible methods to mitigate the vulnerabilities and associated risks.
- Keep themselves updated at all times as technologies are advancing rapidly.

RED TEAM Exercise

A thorough Red Team exercise will test and expose vulnerabilities in a multitude of areas, whereas typical VAPT focuses to exploitation of



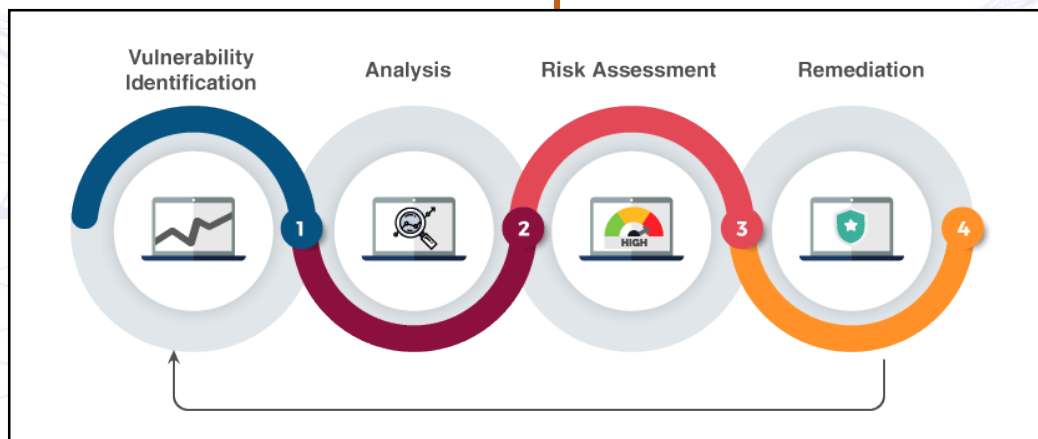
Fig: RED TEAM Assessment Cycle [Ref: <https://sera-brynn.com/understanding-the-red-team-cycle/>]

technical or IT Assets and operation is limited to IT enabled systems. Typically, Red Team operation focuses on:

- Technologies: Networks, applications, routers, switches, databases, appliances etc.
- People: Staffs, contractors/vendors, departments, business partners, supply chains etc.
- Physical: Office areas, buildings, warehouses, substations, data centers, power facilities etc.

response strategy and accuracy to the threats.

- Actual security posture within the organization by initiating real life attack scenarios like as social engineering, phishing and other technique.
- An overview of how the systems secure and responds to any attacks in regards to C2C communication establishment and persistence to the network.
- An assessment result on the physical security strength and access control effectiveness within the organization.



For the large organizations having lots of IT assets, application and also affordable to having dedicated team to detect vulnerable and stealthy points within the organization as-well-as organization's assets/ applications, this is recommended to exercise RED Team assessments to discover and exploit the weakest links to the enterprises. Red Team assessments may provide:

- Simulation of Internal & External attacks and tests the organization's

- Finally, understanding of the defense mechanism as-well-as offences and in a more realistic understanding of risk associated to the organization.

References

- NIST SP 800-115 (<https://csrc.nist.gov/publications/detail/sp/800-115/final>)
- PCI Penetration Testing Guidance: v-1.1 (https://www.pcisecuritystandards.org/document-s/Penetration-Testing-Guidance-v1_1.pdf?agreement=true&time=1602570272621)
- PTES (http://www.pentest-standard.org/index.php/Main_Page)
- OWASP Testing Guide v5



Things to know about Security Intelligence

Rubayet Bin Modasser, Digital Forensic Analyst

Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Security Intelligence is the collection, evaluation, and response to data generated on an organization's network undergoing potential security threats in real-time. This platform was developed from log management, SIEMs, NBADs, and network forensics. As cybersecurity threats and attacks continue to grow and evolve, advanced security solutions are more important than ever, with security intelligence leading the way.^[1]



Key Principles

- Real-time analysis
- Pre-exploit analysis
- Collection, normalization and analysis
- Actionable insight
- Scalable
- Adjustable size and cost
- Data security and risk

Threat intelligence

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

Things about security intelligence

From the context of cyber risk, threat intelligence is considered to be highly potential to help organizations make better security decisions and reduce cyber risk. Intelligence and security teams are often complementing each other, and intelligence outputs can lack relevance to the audiences they serve. It causes slower response to intelligence while it comes at all. This is the scenario where elite security intelligence comes in.

Security intelligence works as the application of intelligence across the security functionality within the organization and beyond. It enhances organizations capacity to realize operational improvements and reduce cyber risk by embedding intelligence into security within their workflows.



Empowering the decision-makers

People in operational and leadership positions mostly makes decisions based on their own expertise and experience. They have limited access to insights that would improve the outcomes of their decisions. Any data on security intelligence puts insights that have historically been out of reach directly into their hands.

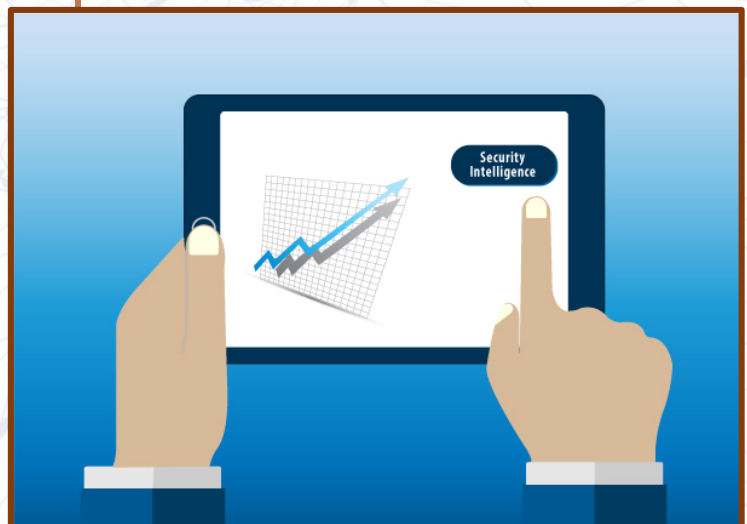
A modern, well equipped and powerful security intelligence solution is well equipped to collect data from a broad range and variety of sources and uses powerful analytics to turn previously unusable information into genuine insights that put impacts on business decisions. Such solution uses natural language processing to ingest information in any language and provide insights in the user's native language.

Dozens of potential sources could be found in dark web, those may have very useful insights, but it'd unwise and potential threat if people go digging around there in search of intelligence. For an analyst a security intelligence solution breaks down the barriers to access these insights, making it safe and easy to pull out the benefit from them.

Turning security into a business driver

In "The Risk Business" the author Levi Gundert discussed on demonstrating return of investment for an effective program for calculating and tracking cyber risk. To forecast the financial impact of cyber incident, security intelligence plays the most integral role and also makes itself essential for a risk-based Cybersecurity program.

Most organizations considered cybersecurity a cost center — a function that consumes a lot of resources without contributing to the bottom line. Outcomes from security intelligence impacts on enabling cybersecurity teams to demonstrate business value in the form of ROI.



Security intelligence is more worthy while it identifies relevant issues & produces more insights regarding business of the organization. Such insights, or intelligence other hand,



supports fast, informed & efficient decision making throughout the organization.

Turning jobs in easy way

Integration with existing technology is a critical step for security intelligence solution providers. So any solution that integrates with existing technologies, providing insights to inhabitant operational staff would be considered efficient. Such efficiency will reduce any extra effort or procedural burden while making a decision. Gavin Reid (CHIEF SECURITY OFFICER, RECORDED FUTURE) says, "Good detection tools get made great with useful, time-sensitive, and low false-positive indicators. A constant stream of fresh insights will help you make the best use of Netflow, DNS, IDS, and all other detection sources."

Alerts from detection tool helps analyst to identify an attack, better if possible to identify in early stage. But challenge comes while prioritizing the alerts. Security intelligence solution integrated with existing technology enriches all the alerts with contextual information. Also makes it easier to identify and high-risk alerts are prioritized.

Making risk relatable for everyone

It is essential to communicate Cybersecurity issues in a language the business understands. Effective security intelligence makes cyber-risk relatable for any audience. It also improves understanding the meaning of threats or insights for the business. Maggie McDaniel (VP RESEARCH FROM INSIKT GROUP) says - "Someone who needs to make a business decision doesn't need technical details. They need to know the 'so what?' of the threat so they can make an effective decision."

An effective security intelligence is solely prepared for its particular target audience. For security analysts this includes technical details and indicator. Although, for an executive, it means a simple definition of the threat and its impact on the organization as well as on business. For a developed cybersecurity function, it must communicate in a



language that is understandable in the



term of business. In other sense we also can define this as “The Language of Risk”.

In a business-focused Cybersecurity function the security intelligence plays the role of a powerful tool. It translates technical security issues in to clear, concise, risk-based insights. As a result anybody can use such knowledge to improve their decision making ability. “Not all insights are useful to everyone. It’s important to have a flexible security intelligence solution that can produce insights in a format and level of detail that’s appropriate to each audience.” — Wendy Swank (SENIOR SOLUTIONS ARCHITECT, RECORDED FUTURE).

In Closing

It requires careful planning while serving different audiences with security intelligence. From security intelligence an operational team may require constant stream of insights from existing workflow. On the other hand, leaders and executives may prefer monthly summaries.

To build an effective security intelligence few question toward the audience may get some help, such as, “what data do you need?”, “where do

you want the data to live?”. These answers will help to determine the format and frequency of intelligence and such security intelligence will provide insights to make more effective decisions.

Having security solution added with threat intelligence helps organizations prioritize their security activities. Security intelligence has to be adaptable enough to be merged with existing & new technologies. This will impact on decision making effectively.

Reference

1. <https://www.exabeam.com/glossary/security-intelligence-definition/>
2. <https://securityintelligence.com/definition-security-intelligence/>
3. https://www.recordedfuture.com/security-intelligence-secrets/?utm_content=140682332&utm_medium=social&utm_source=linkedin&hss_channel=lcp-678036
4. <https://www.forcepoint.com/cyber-edu/threat-intelligence>
5. <https://www.getfilecloud.com/blog/2018/11/a-brief-overview-of-threat-intelligence/#.X41RTtAzbIV>



WSIS Prizes 2020 - SUCCESS STORY

Tanimul Bari, Senior Technical Specialist
(Software & e-Service)
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Bangladesh National Digital Architecture (BNDA) team achieved the WINNER award in WSIS (World Summit on the Information Society) 2020 for the e-recruitment platform (erecruitment.bcc.gov) in the e-Employment category. Haolin Zhao, Secretary-General of the International Telecommunication Union (ITU), announced this at the "WSIS Forum 2020 Prizes Awards Ceremony" held online on 7th Sep 2020. The World Summit on the Information Society (WSIS) Award is considered one of the international recognition in the field of



information technology. The World Summit for Information Society is working to make people's lives easier and change through information and

communication technology. At the same time, the organization is working relentlessly to spread innovations around the world. This article contains success story of winning in WSIS 2020.

Background Information

Over the recent years, BCC has established National Data Center (NDC) for hosting all the government websites, e-mail services and web applications. In the near future, NDC is envisioned to be the only Gateway to access internet services for all of the government organizations. BCC in its endeavor to further progress on its ambitious objective had established Bangladesh National Digital Architecture (BNDA). The aim for this initiative was to create a digital ecosystem within the Government of Bangladesh that provide digital services:

- Seamlessly
- Integrated
- Digitally inclusive
- Strategically Aligned

Project's description (activity's description)

The concept of shared platform/services to facilitate citizen service delivery utilizing emerging



technologies is a crucial part of Bangladesh National Digital Architecture. It ensures cost reduction and optimization is achieved while improving process, information systems and technology support in a disciplined manner. Bangladesh Computer Council established this System as a shared service for all govt agencies. It enables the Govt agencies to accomplish end-to-end recruitment process and related tasks through increased interoperability, enhanced security measures, reduced risk and lower procurement costs.

It's a web based secure system to process recruitment management activities electronically. It covers activities from Job posting to shortlisting of candidates. There is facility to manage Question Bank and online exam. It contains Provision of Online transaction verification with Bank. It's integrated with DLS platform (a private Blockchain infra) for storing admit card info. It has 3 modules – e-Recruitment module, Exam Controller module and Online Exam module

Results achieved:

This Recruitment Management System is a successful project based on implementation achievements. It has been used by 26+ Govt

agencies/projects. Recruitment of 1900+ applicants is already completed! It has processed 1,70,000+ online job applications against 75+ posts of 65+ different recruitment notices in last 2.5+ years. Several entities have used this system multiple times. 2-3 new agencies are in pipeline.

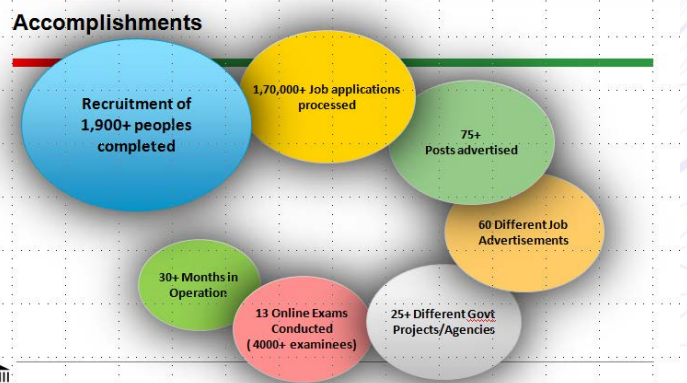






Figure 6: Usage Statistics of Shared Recruitment Management Service

Impact:

ICT ministry has decided to launch National Govt Jobs Portal based on this shared service. It has helped agencies to process large number of job applications within shortest time & effort and enable agencies to focus on their core functionalities. We are seeing impressive response from govt organizations and applicants. It's saving govt expenditure to a great extent as they no longer need to procure similar system. Job applicants from rural areas are now able to apply with ease and relieving them from standing in queue in bank branch. It's creating positive impression among applicants about govt services.



Examples of linkages between the WSIS Action Line your project was awarded for with each of the Sustainable Development Goals it helps advance

| WSIS Action Line | Sustainable Development Goals | Project Benefits Realized |
|------------------|---|--|
| e-Employment |  | The shared Recruitment management Service is enabling Government agencies to deliver integrated citizen services to all classes of citizens : Rural, Semi-Urban and Urban. Also it's enabling poor people to apply for govt jobs from home using mobile |
| |  | BNDA and e-GIF compliant Shared Recruitment management Service is enabling transparent recruitment for Government of Bangladesh. |
| |  | The Shared service for recruitment process management is enabling poor and rural people to apply for govt jobs with a fair opportunity to be selected (if found competent). |
| |  | The shared service for recruitment process management has provision of applying job application and taking exam online, thereby alleviating usage of paper and conserving environment. |

Social, economic, and environmental impact of the project

Social Impact:

Recruitment Management System has some social impact also. Online exam facility ensures fair judgment, fair competition and impartial behavior, thereby creating social values. Again Blockchain enabled Admit card prevents forgery and collusive practices, hence ensuring social norms.

Economic Impact:

It provides huge savings (max 90%) in effort spent for scrutinizing job applications and shortlisting candidates based on criteria. Also, it helps govt organizations to expend less in recruitment management activities by utilizing this shared service. BCC has already provided services equivalent of several Crore BDT to govt agencies.

Environmental Impact:

This citizen service has direct impact on environment. It is in-line with 'Go Green' initiative. In manual recruitment process, an applicant has to submit piles of papers, documents, copies of certificates, recommendation letters and so on. Our recruitment management system is enabling applicants to submit job applications electronically. Also, it has provision of taking exam online, instead of pen and paper based exam, with automatic result processing facility. So it's removing use of paper and printing to a great extent. And thereby having positive impact on environment.

Highlights of the project's partnership activities

| SL No# | Department/ Ministries | Role | Mode of Interaction |
|--------|-----------------------------------|--|----------------------|
| 1 | ICT Division | <ul style="list-style-type: none"> Guide and Monitor Project progress Assistance to get coordination/response from line ministries | Periodic |
| 2 | Bangladesh Computer Council | <ul style="list-style-type: none"> Provide strategic and tactical support to continue the system operation Provide hosting space and deployment infrastructure Provide Support to solve technical issues Facilitating approval of all the technical documents like <ul style="list-style-type: none"> Functional Requirement Specification System Requirement Specification | As and when required |
| 3 | Ministry of Public Administration | Provide Recruitment related rules, regulations, form, template etc | As and when required |

Challenges and project's future perspectives

Challenges:

1. Regular review of Question bank: The question bank was established in collaboration with academic institutions. However, the question bank needs a regular review and update mechanism to cope with contemporary issues. Otherwise, it may negate the advantages already gained by usage of the service.
2. Security of question bank: The question bank is maintained electronically as part of the system. There is always risk of hacking and cracking activities with the question bank by vested quarter to get unsolicited privileges.
3. Online Exam in large scale: The system has provision for taking online exam. However, it will require large exam center with many computers & internet facility. As a result, conducting online exam in large scale is a great challenge in our country.

Future Perspective:

ICT ministry has decided to launch National Govt Jobs Portal based on this shared service. Talks going on with Public service commission (bpsc.gov.bd) to utilize the shared service. BNDA team is also trying to improve system scalability, User experience, security features and so on. ICT Ministry is developing GRP (Government resource Planning) software to be used by govt agencies. This recruitment management service will be integrated with HR module of GRP software – such type of decision is already taken by BCC. We have plan to introduce insights and analytics in the system. We have plan to incorporate SMS sending feature with the portal. Again to improve User Experience BCC is planning to employ ML (Machine Learning) technique in the system. The system will utilize ML technique to find closest matches with the qualifications & experiences mentioned in recruitment notice and notify those job seekers about new opportunities. The recruitment management service will be integrated with more mBanking service provider so that applicants can do the payment with his favorite mBanking service provider. We hope it will act as one stop solution for any type of Government recruitments in future.

Conclusion

We assume WSIS Stocktaking and WSIS Prizes contest as an effective one to promote any govt/non-govt organization's development aspects. It's also enables creating healthy competition among govt/non-govt organizations of same country in terms of innovation, excellence and citizen service delivery. We wish every success of WSIS Stocktaking and WSIS Prizes contest. Also, BNDA Team is preparing to participate in WSIS 2021 also. Hope more Bangladeshi project will get recognized in WSIS 2021.





BGD e-GOV CIRT

CYBER THREAT INTELLIGENCE

BGD eGov CIRT in association with global partners receive various threat intelligence through relevant sources. These threat intelligences may be subscribed by CIs, Banking and Financial Institutions for assuring cyber security in their domain.

- ♥ Threat Intelligence will be provided to the entities such as Critical Information Infrastructures, Banking and Financial Institutions, Law Enforcement Agencies etc.
- ♥ Domain /entity based threat received from multiple sources will be provided on monthly basis.
- ♥ Critical threat intelligence will be shared as and when received.
- ♥ This service is purely on subscription basis.

BDT 1,00,000 per month.

Minimum Subscription for 1 (one) year.

BDT 1'00'000 per month



ICT Tower, E-14/X, Agargaon
Dhaka, Bangladesh.



info@cirt.gov.bd



+8802 5500 7183



**ICT
DIVISION**

FUTURE IS HERE



**Bangladesh
Computer
Council**