Cybersecurity Scenarios in the Post Covid-19 Situation

Amid the spread of Covid-19 global pandemic, government and industries in different nations are working collectively to address the global humanitarian challenge, support victims and develop an effective vaccine. Businesses around the globe are rapidly adjusting to the changing needs of their people, customers and suppliers, while navigating the financial, operational and cybersecurity challenges. Businesses and organization across the globe are adopting to remote access, work/learn from home policies and endpoint security on a massive scale. In this post Covid-19 world, cybersecurity is emerging as a core technology for companies and institutes to secure themselves when millions of employees start working from home. Companies now understand the risks associated with their data security and data privacy. They are looking forward to IT disaster recovery and contingency plans that can covers all possible types of fabricated attacks during the rapid emerging outbreak of Covid-19.

According to a study by "Centrify"[1], 71% of UK based corporates believe that in the Covid-19 crisis, shifting to 100% remote working has made enterprises more vulnerable to cyber-breach. A statistic released by "State of Cloud Security" and the survey conducted by Fugue Inc.[2], states that 84% companies are worried about cloud security during Covid-19 crisis. 84% cloud engineers are worried about "new security vulnerabilities created during the adoption of new access policies, networks, and devices used for managing cloud infrastructure remotely."

The biggest threat companies are facing post Covid-19 is the rapid enablement of remote work access to critical information at lower security standards. In India[3], Ministry of Electronics and Information Technology (MeitY) have joined hands with DSCI (Data Security Council of India) to establish a National Centre of Excellence for make India an attractive cybersecurity market by accelerating cybersecurity innovation. They hosted the "*Security Investors Conference*" to accelerate funding and brought together key government stakeholders, multinational investment firms and around 70 cybersecurity start-ups and large enterprises on the same platform.

[1] https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#575adf6a381d

[2] https://solutionsreview.com/cloud-platforms/fugue-84-percent-of-companies-worry-about-cloud-security-during-covid-19/

[3] https://www.news18.com/news/tech/cybersecurity-in-india-to-witness-high-demand-post-covid-19-pandemic-2574425.html

Network Security

Many remote devices lack even basic network security. According to Natali Tshuva[4], CEO of IoT security company Sternum, hackers during post Covid-19 crisis are targeting remote monitoring and medical devices, which could be dangerous, even lethal, for users and organization.

Key challenges in network security during Covid-19 crisis are:

- **Migration from monitored to unmonitored network:** Immediate migration to personal network of employees has exposed organizations to a higher risk of phishing and network attacks via fraudulent websites and phishing emails by hackers preying on anxious human nature related to coronavirus.
  - As Mr. Marc Rogers[5], V.P of cybersecurity strategy at Okta and Defcon's head of security said – *"spear-phishing email attacks related to COVID-19 have increased by 667% since the end of February 2020 and a similar phenomenon is observed in other nations as well".*
- **Lack of IT resources:** For a secure remote access strategy, institutes such as schools, colleges lack in special configurations requirement for their proprietary, on-premise software to access remotely.
- **Providing secure remote access:** Most SMBs in India use internal network as their IT architect, such organizations face challenge in providing their employee/user a secure way to access those systems via a VPN or other networking solution. Also, government and regulated industries such as legal, insurance, banking use systems, devices that are not approved for massive influx of remote workers and faces significant cyber threat.

Cloud Security

The sudden shift to a remote workforce has altered IT priorities and initiatives of CIO from various enterprise. According to the survey conducted by Adobe[6] in mid-March, most CIO in U.S are expecting to increase their financial investments in security technologies. Public cloud, infrastructure, and AI and ML will also receive financial boosts in many organizations.

Key challenges in cloud security during Covid-19 crisis are:

- Many organizations are using public cloud service to some degree, but most of their data is housed on-premises. Hence offering challenge to companies to operate from remote location.
- Cloud engineers are facing challenge to keep their enterprise's cloud solutions secured due to distribution of team with remote access. According to Fugue's CEO Mr. Phillip Merrick – "Cloud

[44] https://www.zdnet.com/article/telehealth-whats-at-stake-from-a-security-standpoint/
[5] https://www.capgemini.com/wp-content/uploads/2020/04/Cybersecurity_2020403_V05.pdf
[6] https://www.zdnet.com/article/how-remote-work-is-changing-cio-priorities-amid-the-covid-19-pandemic/

misconfiguration not only remains the number one cause of data breaches in the cloud, rapid global shift to 100% distributed teams is creating new risks for organizations and opportunities for malicious actors."

- High demand in cloud-based applications has enabled a global, interconnected workforce via different cloud systems, making challenging for organization to determine whether the authenticate user have access to information.

User Level Security

In India, Kerala being the worst-hit states in Covid-19 crisis, the database of all confirmed and quarantined patients was handed over to the police and the district health administration to help them in continuous monitoring of respective individuals. However, the same list started appearing locally on various social media groups and forums. This is a severe breach of personal data as proposed in India's Personal Data Protection Bill 2019. Also, on March 8, 2020, the State Health Department's eHealth portal was attacked by a hacker group known as 'GhostSquadHackers.

Key challenges at user level security during Covid-19 crisis are:

- **Lack of a centralized, authoritative IAM repository:** Lack a centralized database to effectively manage and secure user identities and data infrastructures during post Covid-19 period.
- **Unauthorised user network:** Companies are facing a constant risk of vulnerability to their databases due to the queries such as "Do employee/user have secured home Wi-Fi network", "What mechanism do they follow to secure their personal computer".
- **High dependency on mobile devices:** Mobile cyber-attacks on platforms like SMS, iMessage, WhatsApp, and others, trigger immediate responses from recipients. High dependency on mobile devices by students and employees during learning/working from home is another area of concern for an organization during crisis.
- **Data leakage and Lack of endpoint security solutions:** Organization face challenge of data leakage due to usage of unapproved USB and media cards at home computers. They also face a challenge to control and monitor user activities due to non-installation of proper endpoint security and antivirus solution at user device.

Best Practices for Remote Working and Learning

Phase 1:

- **Educate employees on Covid-19 cybersecurity issues and develop comprehensive cybersecurity guidelines for employees working from home.:** Run security awareness campaigns across the organization to educate employees on the cybersecurity challenges they may face as they work from home. As employees may not be able to access internal communications channels via secure VPNs, so establishing alternate communication channels that do not require a VPN is critical to ensuring that all employees receive regular cybersecurity updates.
- **Build or strengthen the remote surveillance and capabilities to detect cyber threat:** Ensuring company-issued devices can be remotely wiped clean in the event of a breach and use of personal devices by remote employee must be prevalent or monitored through a remote desktop application.

Phase 2:

- **Augment cybersecurity capabilities with AI-enabled tools:** Organizations should enable the use of AI to increase security without a massive increase in resources as did by Siemens Cyber Defense Center (CDC) which used AWS (Amazon Web Services) to build an AI-enabled, high-speed, fully automated, and highly scalable platform to evaluate 60,000 potentially critical threats per second
- **Deploy security orchestration, automation and response (SOAR):** SOAR can help organizations to collect security data and alerts from different sources, for incident analysis. It can be very effective in automatically taking actions on the anomalies observed on the endpoint. If it is Laptop enabled with EDR, we can apply Policies to automatically quarantine the machine. Similar actions can be taken for MDM enabled Mobile devices

Phase 3:

- **Collaborate with other organizations to share Covid-19 related cyberattacks:** Organizations should create communities like Covid-19 CTI (cyber-threat intelligence) League which are focused on Covid-19 related cyberattacks and share the latest threat data.
- **Plan for a staggered return to the corporate network and identify potential failure points in the systems and revamp security protocols:** Security controls like VPN might not work efficiently remotely due to high traffic generation. This increases chances of devices to be compromised during Covid-19 crisis. Organizations should screen such compromised devices in a staggered manner with latest anti-virus before connecting then back to their network.

Covid-19 has not only had a stress-tested society and the global economy but is also stress-testing cybersecurity defences of organizations across the industries. It has helped the organizations to identifying glitches in cybersecurity practices and revamp security protocols. Moreover, as companies have now started investing more in building online capabilities for remote access, cybersecurity technology and various cybersecurity solutions will emerge even stronger in the future.

Frequently Asked Questions (FAQ)

Business Continuity

- **Question**: What all is at stake for my business in case of a Cyber Security Attack?
  - **Answer**: A successful cyber-attack can cause major damage to your business. It can affect your bottom line, as well as your business' standing and consumer trust. The impact of a security breach can be broadly divided into three categories: financial, reputational and legal. To prevent from any Cyber-attacks, it is important to build adequate defences. A Managed Security Services Provider would better be able to recommend right mitigations suiting to your IT estate.
- **Question**: What can be the impact of Cyber Security Attack on my Business?
  - **Answer**: A successful cyber-attack can cause major damage to your business. It can affect your bottom line, as well as your business' standing and consumer trust. The impact of a security breach can be broadly divided into three categories: financial, reputational and legal. To prevent from any Cyber-attacks, it is important to build adequate defences. A Managed Security Services Provider would better be able to recommend right mitigations suiting to your IT estate.
- **Question**: Do you consider outsourcing a managed detection and response management, to mitigate the possible risk of cyber threats while remote working (lower staff to handle request/ expert supervision)
  - **Answer**: Managed Detection and Response is well suited to small and mid-sized organisations. Depending on the scope of cyber protection needed, sometimes a full-fledged MDR may be over kill and a costly affair. A due diligence need to be conducted by talking to an MSSP.

Cloud Security

- **Question**: How do I protect sensitive information handled & stored by third party vendors?
  - **Answer**: Encryption of the Data, Good Governance on 3rd party managed systems, Regular Audits are key for Data Protection in a 3rd Party vendor managed environment. An MSSP will be able to guide you through insights into each of these areas.
- **Question**: Do I need to worry about the security of the applications, software or cloud-based storage system that I use?
  - **Answer**: Business critical Applications, Databases, Storage etc.; are to be protected irrespective of where they are located, whether On-Premise or in a Cloud.

Cyber Threat

- **Question**: How do I know if my business is under cyberthreat?
  - **Answer**: The Cyberthreat symptoms can be very varied. Malware and Phishing attacks are quite common. Malware attacks show up the symptoms of Slow computer performance, Opening and Closing of programs automatically, Frozen windows etc.; Whereas Phishing attack symptoms would be largely around Social engineering like, Asking for Confidential information, Use of urgent threatening language etc.; It is highly advised to talk to a Cyber Security Specialist when faced with any of the above symptoms.
- **Question**: Can data governance strategy minimize cyber risk?
  - **Answer**: Data Governance is an overarching control over the Policies, Guidelines, Frameworks etc.; However, by mere Data Governance in place, Risks cannot be reduced. It needs a strong People, process and Technologies in place along with a decent education and awareness around IT Systems. Pl consult an MSSP for further guidance.
- **Question**: What are common types of cyber-attacks I should know?
  - **Answer**: The Cyberthreat symptoms can be very varied. Malware and Phishing attacks are quite common. Malware attacks show up the symptoms of Slow computer performance, Opening and Closing of programs automatically, Frozen windows etc.; Whereas Phishing attack symptoms would be largely around Social engineering like, Asking for Confidential information, Use of urgent threatening language etc.; It is highly advised to talk to a Cyber Security Specialist when faced with any of the above symptoms.

Cyber Training

- **Question**: How do I train my team, so they know what a cyber-attack looks like?
  - **Answer**: ISO 27001 offers a good guidance on user awareness and education on general Cyber security issues. In case, you are not doing a ISO 27001 assessment, then you can consult an MSSP to help you guide on creating a Cyber Security awareness, the associated programs.

Network Security

- **Question**: What should be my bare minimum resource allotment to tackle cyber threats?
  - **Answer**: We have to look at protecting the organisation from cyber-attacks, in a comprehensive manner. People, Process and technology are the three pillars that constitute the framework. Depending on the Assets to be protected, we will have to fine tune the balance among three pillars. An MSSP will be in a better position to guide you further.

- **Question**: What are the minimum basic requirements that I should take care so that my company's network is not compromised to cyber-attacks?
  - **Answer**: Perimeter Security like Firewalls, DDoS, WAF etc.; will prevent from external attacks. Controls like IPS, internal firewalls protect the internal systems. Security principles like "Least Privilege", Segregation of Duties, PAM controls would prevent unnecessary outages.
- **Question**: We have recently started taking customer payments through online transactions. I am worried about the online scams. How do I protect myself?
  - **Answer**: Online Payments are dictated by PCI DSS Compliance. PCI-DSS has elaborate guidance and comprehensive security controls to ensure safe and secure online transactions.
- **Question**: What measures have you considered to limit mass mail entries into your email network (Unsolicited/ Spam emails/ network traffic)
  - **Answer**: Unsolicited mass e-mails are restricted by the use of Anti-Spam solutions that many e-mail security solutions offer by default these days.
- **Question**: Are you prepared to handle operation risk of supporting large number of VPN Connections simultaneously? (Available infrastructure, IT workforce)
  - **Answer**: A Managed Security Service Provider has a bulk of Licences in hold. Also, MSSP will be in a position to augment the capacity very quickly. Therefore, talk to a sound MSSP who offer Network Security Solutions.

Security Auditing

- **Question**: How can I perform my organization's risk assessment?
  - **Answer**: Assessing and managing risk is a high priority for many organizations. Given the turbulent state of information security vulnerabilities and the need to be compliant with so many regulations, it's a huge challenge. Depending on the type of Assests and its associated Risks in terms of both Qualitative and Quantitative, an MSSP can guide you through the relevant framework for your Organisation.
- **Question**: How do I remain updated in the cyberthreat landscape?
  - **Answer**: Many MSSPs offer a Threat Intelligence advisory contextualised to your Assests. Also, you can subscribe to a Global Threat Intelligence feed from an MSSP. Besides this, you also have to update your systems with appropriate patches and regular hardening of systems.
- **Question**: What does my company need to do to ensure cyber security keeps moving forward (the current process/practices/tools keeps on improving)?
  - **Answer**: Cyber Security posture management is an on-going process. Have a good GRC tools to measure the Risk Score time to time. Also, tune the systems for patching, VA etc.; by

adopting to a good analytics tool that gives insights into what is working and what is not. An MSSP will be in a best position to offer you right guidance.

- **Question**: How do I minimize the effect of a cyber-attack? What practices will help me cushion the impact?
  - **Answer**: Training the employees in cyber security principles, Install, use and regularly update antivirus and antispyware software on every computer used in your business, Making backup copies of important business data and information, Controlling physical access to your computers and network components is just some of the best practices.

Security Compliances

- **Question**: What can I do to protect my business from Cyberthreats?
  - **Answer**: Cyber risk assessment involves identification, analysis and evaluation of cyber risks. As part of the assessment, you should look at your entire IT infrastructure and try to identify possible threats arising from internal and external actors. Basis the outcome, you have to plan for Protection, detection and Response controls. A Managed Security Services Provider would better be able to recommend right mitigations suiting to your Key assests.
- **Question**: How effective are the free or cheap antivirus software?
  - **Answer**: Now-a-days the cyber-attacks are sophisticated. The easy entry point for a cyber-attack is to compromise an end point and further escalating the privileges. Therefore, any cheap, non-standard AV will have very detrimental effect on the Organisation. Pl reach out to an MSSP for further guidance on the same.
- **Question**: Do I need to train my staff for cyber security?
  - **Answer**: Skilled and Knowledgeable cyber security staff is on Demand these days. Therefore, while critical Business systems can be managed in-house, specialised cyber security can be outsourced to an MSSP. A good GRC manager on-site would be able to manage the GRC for internal purposes and also the MSSP.
- **Question**: What best practices should I follow in my company?
  - **Answer**: Regular Patching of systems, Applying Global Threat Intelligence, Continuous monitoring and managing of systems for internal as well as external threats are very few out of a large set of Best practices. An MSSP will be able to manage the environment for you by adhering to Global best practices.
- **Question**: What is Cyber Insurance?

  - **Answer**: Cyber security insurance can help your business mitigate risk exposure by offsetting some of the costs involved in cyber incident recovery. Pl speak to an MSSP for better understanding the Incidents covered around the same.
- **Question**: Are there any mandatory regulatory compliances that I need to follow?
  - **Answer**: Regulatory compliances are dictated by the Industry you belong to and the constraints in terms of complying to them from your Customers, Business associates etc.; Typically, HIPAA is used in health Industry, PCI DSS I Payment Industry etc.; An MSSP will be in a best position to guide you further.
- **Question**: How can I measure my cyber resilience? Or how can I measure my level of preparedness for any cyber-attack?
  - **Answer**: Red team exercises, Breach simulation exercises will give great insights on sudden and unknown attacks. Whereas Penetration tests and Vulnerability assessments will help set a regular discipline and basic hygiene for systems.
- **Question**: Is there a Cyber Essentials themes/requirement which my organization can follow/adhere to reduce majority of the attacks?
  - **Answer**: Cyber Essentials or Cyber education will help to take an informed call. However, Gap assessments, Audits and Cyber drills are true testament to the posture management. Therefore, Cyber education will offer great help in appreciating various Cyber assessment tools and subsequent actions needed on the part of organisation for cyber preparedness.
- **Question**: Does IT practice patching often to ensure low risk of window breaks by attackers (software updates/ bug fixes/ vendor management/ password change)
  - **Answer**: Certainly, Yes. This is a best practice indeed. However, with the emergence of Zero-Day attacks and they are becoming too common these days, these best practices alone may not be a fool proof method.

User-Level Security

- **Question**: We had to allow to some of our employees to use their personal computers at home to carry out their regular business activities. How should I ensure that they don’t compromise the integrity of my IT landscape?
  - **Answer**: Technology has evolved and a " Zero Trust " Philosophy guides the fact that " Don’t trust but verify ". With this in mind, it does not matter whether the device accessing the Applications is inside or outside the organisation. Just that adequate controls have to be in place to support Zero Trust Framework.
- **Question**: How can I determine the right controls and policies for my organizations systems?

- **Answer**: A thorough Gap Analysis will reveal various gaps in the system. Appropriate controls can be implemented based on the Risks perceived and the IT budget. Gaps will also be lead indicators for IT Policies.

- **Question**: If my organization is using mobile devices for work, am I prone to cyber-attacks and risks? If yes? What are the best ways to tackle such situation?
  - **Answer**: As long as appropriate office controlled in the form of Mobile Device Management software is installed, an Acceptable Suer Policy is established, there will not be an issue. The security solutions for such devices must be planned by organisations in advance to prevent any cyber-attacks. You may reach out to an MSSP for supporting such solutions.
- **Question**: I am using my personal device for remote working. Is it prone to cyber-attacks?
  - **Answer**: As long as appropriate office-controlled software is installed and enabled on your personal device, there will not be an issue. The security solutions for such devices have to be planned by organisations in advance to prevent any cyber-attacks.