CYBER CRIME, CYBER RESILIENCE AND SECURITY STRATEGY IN POST PANDEMIC WORLD

By Lawanya Singh
From Chanakya National Law University, Patna

Abstract
Digitization of businesses is the most anticipated move post COVID-19 where the Indian companies may also be seen devising robust cyber security plans. While Lockdown taught us the importance of online tools and media, it threw a much needed light on the need for cyber security. Surge in cybercrimes across India shows data vulnerability and uncovers our unpreparedness. With businesses resuming their work, the need for devising post COVID strategy to manage cyber security is compelling. Fostering a culture of cyber resilience and focusing on protecting the organization's critical assets and services should be the starting point. Classic perimeter and endpoint security provide little protection here, other technologies, like encryption, data loss prevention, and even cloud applications could help reduce such risks. With work from home becoming a new normal, employees using their own systems unequipped to handle cyber-attacks increases the risk of losing critical data. Therefore companies may require to set up their own secured channel through which company’s data flows together with employee end devices laced with security requirements suited to its need combined with more utilisation of cloud based storage. Working from home also means companies can no longer monitor the activities carried out by the employees on the company’s behalf thereby increasing the possibility data breaches caused by exfiltration rather than infiltration. Further, a risk assessment of company’s security could save it from data breaches. Incorporating cyber-security technologies is an expensive affair making corporate giants leaving behind the cash crunched Small and Medium-sized Businesses in post pandemic cyber security management.

The paper aims to highlight potential risks of cybercrimes faced by businesses and ways to mitigate it. It also focuses on the challenges of working remotely, effectiveness of cloud-based storage and how a combination of security tools, response plans, awareness training, and education could make both big and small businesses more defensible and less likely to suffer from data breach and cyber-attacks post COVID-19.

Keywords: exfiltration; cloud storage; cyber resilience; employee training; remote working

INTRODUCTION
Cybercrime may be defined as “Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime”. Forms in which these may take place includes impersonation and identity theft, Ransom ware, Computer Virus, Worms, Trojan horse, Website Defacement, Denial of Services (DoS) attack, Cyber-Squatting, Pharming, Crypto jacking, Espionage.

National Crime Records Bureau released a data in 2019 where a 77% rise in the number of cybercrime cases was observed in 2017 compared to 2016\(^2\), showcasing constant rise of cybercrime within India. The data is of 2017 meaning this growth percentage could have reached new heights till present year. A surge in crime was observed even during the period of nationwide lockdown putting many businesses into realisation of cyber-attacks being a dangerous threat and chances of them facing these attacks is not inevitable. For a tech aware city like Bangaluru to have highest number of reported cyber-attacks cases is surprising but on second thought it is understandable that knowledge, information and awareness about cyber crimes are the attributable reasons to higher reporting making us question the position of other states in India.\(^3\)

With corporate sector all set to resume its business post prolonged lockdown period, the need to devise a strong cyber security strategy is compelling than ever. Covid-19 itself was used in attacking corporate sector. For example, COVID-19 was cited in fraudulent e-mails as a reason for delayed shipments or the need to reorder. The authors marked the e-mails as urgent and required to check attached files immediately. Another way of attacking the system with Trojan horse was by asking the recipients through mail to fill out a form otherwise their company would be shut down \(^4\). All these incidents points to one single thing: need for cyber resilience.

A Frost & Sullivan study commissioned by Microsoft revealed that a large-sized organization in the Asia Pacific region can possibly incur an economic loss of $30 million, more than 300 times the average economic loss for a mid-sized organization. This is more than seven percent of the region’s total GDP of $24.3 trillion.\(^5\)

The Study also examined the current cyber security strategy of organizations in India. It found that for organizations that have encountered cyber security incidents, remote code execution and data exfiltration are the biggest concerns as they have the highest impact with the slowest recovery time. A large number of cyber security tools and a complex environment also add to the turnaround time. Most organizations lack a cyber-security strategy, while for a large majority cyber security was an afterthought. About 59% of respondents accepted that the fear of cyber-attacks has hindered digital transformation projects. 37% see cyber security strategy only as a means to safeguard the organization against cyber-attacks rather than a strategic business enabler. A mere

---


18% seeing cyber-security as a digital transformation enabler.\(^6\)

Widely available information regarding cyber-attacks relate to data infiltration i.e. Information on how attackers get past security defences and into the network but a real risk to most of the organisation is data exfiltration i.e. removal of data by the attackers. With increasing sophisticated attacks, poor security practises make it more challenging for the company to protect their data. When it comes to stealing corporate data, almost two-thirds of the breaches involved traditional corporate networks, and cloud break-ins accounted for the other third.

As networks and cloud environments stretch to accommodate the new reality, edge security strategies must be extended. Companies were quick to realise the need to change their infrastructure and workspace pattern during Covid-19 outbreak and half of firms fear an increase in cyber-attacks as a consequence of changed working patterns.\(^7\)

Many companies that had already invested in integrating their software-defined networking in a wide area network (SD-WAN), next-generation firewall (NGFW) technology and multi-cloud deployments into a unified system were in a much better position to pivot to the demands of a totally restructured workplace. Post-COVID-19 remote networks have taken a primary position, requiring organizations to extend strategic edge approach throughout the network and out to the cloud to make sure it is consistent, integrated and secure.\(^8\)

The relatively high success rates of cyber-attacks show that organizations often fail to implement proper segmentation controls. Failure to do malware scanning after infiltration into the network allows hackers to easily move from one machine to another. Hackers find high success rate by using simple techniques like DNS tunneling, or trickling data out within packet headers to slowly steal data without raising suspicion and this simple technique works most of the time especially in organisations facing financial crunch to be able to employ high end solution. A security firm pointed out that most of its customers have managed to significantly reduce attack success rates simply by optimizing existing security controls.\(^9\)

Data breaches can happen to any business. But, with insight, intelligence and the right technical solutions, chances of it happening could be drastically reduced.\(^10\)

---


\(^8\) Ken Xie, June 2, 2020, we must rethink and repurpose cybersecurity for the covid-19 era https://europeansting.com/2020/06/02/we-must-rethink-and-repurpose-cybersecurity-for-the-covid-19-era/.


Continuous network monitoring and DLP technology displayed a strong correlation with improved security posture and breach detection. No single tool or technology will solve all data security problems but non-deployment of data loss prevention technology could have prevented past data exfiltration especially in the commercial organisations that were less likely to install it. Detection of data breaches was possible for organisations which continuously monitor their network for unusual or anomalous behaviour because organisations with no monitoring may never come to know about data breaches. Cyber-attacks are mostly discovered by external agents or companies come to know about them only when attacker releases stolen information. Data\textsuperscript{11} shows that only 39% serious data breaches were discovered by internal security teams in India with medium sized organisations most likely to have them discovered by external agents, perhaps due to growing pains and budget stresses as the IT and security organizations mature.

Both corporate giant and SMBs require a strategy to prevent cybercrimes while it is easy for giants to dedicate large number of resources for combating cyber-attacks but for SMBs challenge continues. There is no dearth of inexpensive choices for SMBs to practise. Therefore a mind-set that “we are not at risk” should be set aside and careful planning and implementation of available and exercisable choices be made.

[1] Changing Infrastructure: Controlling remotely placed employees

Working remotely during COVID-19 was not easy but it taught that changes such as working from home can be an option. If employees work in the company provided infrastructure problem of securing data is not a concern. Most of the people are ill-informed and fail to follow any security guidelines. An example to suit the statement would be using a USB stick in the device used for storing or processing critical data and information. Now the challenge with remote working is inability to control the data that employee processes or stores. Even from the attackers perspective, infiltrating a well secured network is taxing, requiring an in depth knowledge but how hard will it be for attackers to bribe an employee and secure a copy of company’s critical information or using their credential to steal information from cloud based storage. Now at this juncture only an employees’ strong ethics and morality can save the company leaving them with little exercisable choices to prevent such incidents. One preventive measure could be user access control\textsuperscript{12} or data encryption\textsuperscript{13}. Encrypting data at rest or in transit is a common and mature approach to prevent attackers from gaining an access to actual data. Attackers may get access to the encrypted data they will not be able to read the actual data without having access to the

\textsuperscript{12} Doe, N.P. and V. Suganya. Secure service to prevent data breaches in cloud. in Computer Communication and Informatics (ICCCI), 2014 International Conference 2014. IEEE.
required decryption key.\textsuperscript{14} Data theft through Ms. Word was found to be most prevalent.\textsuperscript{15} So restricting its properties: disabling it from being copied unless provided with authentication by the author can save data thefts and will provide an information to the head as to the identity of user asking such authorisation. Unknowing or wilfully using USB sticks can prove dangerous for data safety. Wilson and Lavine\textsuperscript{16} present a discretionary access control method for preventing data exfiltration via removable devices. The authors tie the dissemination of files via USB storage to the classification of a file. Files are appointed a distribution level and community of interest label, which is used to automate the decisions about whether or not to allow a file transfer to take place. Although feasibility of this process is questionable because authorisation of each and every document is difficult but at the same time small sized business could be benefitted.

Ensuring cyber security while working remotely is challenging but practising cyber resilience is key to such challenges. It means organisations should have ability to continuously deliver a desired outcome despite adverse circumstances and events. In addition to systems, services and applications, cyber resilience is concerned with leadership, teamwork and the effort an organization puts into improving its readiness and ability to recover.”\textsuperscript{17} To keep a check on remote computers and devices used for connecting to company’s network. They need to hire ethical hackers to check for potential security threats helping them in getting a better understanding of their security vulnerability and what would be the best way to defend against data breaches. Another practise that should be followed by remotely working employees is to use a Virtual Private Network. A VPN maintains privacy of data through security procedures and tunnelling protocols, in effect, data is encrypted at sender’s side and forwarded via "tunnel" which is then decrypted at receiver’s side. An additional layer of security can be added by encrypting not only the data, but also the originating and receiving network addresses.\textsuperscript{18} Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network\textsuperscript{19}, hence protecting company data from being seen by unauthorized personnel.

\textsuperscript{15} Supra note 11
[2] CHALLENGES TO CYBER SECURITY

[2.1] THREAT FROM GROWING INSIDER MARKET AND SOCIAL ENGINEERING

A study has revealed that phishing/social engineering attacks increased from 48 percent in 2017 to 52 percent in 2018.\(^\text{20}\) Human factor remains a weak link in security, the focus on social engineering will increase with other types of attacks such as that on infrastructure involves lot of skill and time and is expensive making it more difficult to carry out therefore an easier way would be paying huge sum to any insider or simply deploying an agent into the company without that person realising that he is acting illegally.

[2.2] LACK OF KNOWLEDGE AND NEED FOR EMPLOYEE TRAINING

A study by a security solution company has shown that education and experience plays a big role in detection and prevention of data exfiltration. Lack of knowledge and unfamiliarity with a full range of security technologies can be alarming for any company. Therefore businesses should not only focus on bringing in advanced technologies but also training their employees because without having confidence in their ability to safely use data and information, any amount of security solution deployment would be a waste of company’s resources. Businesses should focus on employee security training and developing a security operations centre.

Increasing the frequency of network monitoring for unusual or anomalous traffic from weekly or monthly to at least daily or continuously. Almost 70% of those with five years or more experience monitored the organization’s network at least daily, compared to 57% of those with less than five years of experience.\(^\text{21}\)

[2.3] INCONGRUITY BETWEEN EXECUTIVES AND SECURITY EXPERTS

One of the greatest challenge is ensuring that all of the decision makers of the company are on same page because only then a healthy cyber security budget can be put in place. Data breaches can be directly attributed to lack of internal collaboration. Studies of recent data breaches reveal that 70 percent of breaches are actually caused by people and process failures within the company. Contrast this with the fact that 60 percent of C-level executives believe that their current company solutions protect them well enough against hackers, v/s only 29 percent of IT pros who believe the same. In fact IT professional also feel lack of support from executives in promoting for enhanced security technology. Still many companies rely on reactive rational to fight data breaches instead of investing in solution which is advanced enough to combat emerging threats.\(^\text{22}\) Also there is a lot of confusion regarding who is responsible for handling cyber security in a company. A study by Keeper Security revealed 33% believe company leadership is responsible for cyber


\(^{21}\) Supra note 11

security. Few (9%) believe cyber-security is the responsibility of individual employees. 62% of CEOs, chairs and business owners believe they (company leadership) are responsible for their company’s cyber-security. Only 14% of group/team heads think company leadership is responsible and instead believe it is the responsibility of a dedicated team (51%). While 37% report having a dedicated IT or cybersecurity team. Therefore proper understanding of responsibility could save company from major data breaches.

[3] SECURITY STRATEGY FOR SMALL AND MEDIUM-SIZED BUSINESSES

Cyber-attacks on small and medium-sized businesses (SMBs) have been on the rise. According to a 2019 study by Accenture, 43% of cyber-attacks worldwide are aimed at SMBs. India has 6 crore SMBs that account for 30% of the GDP as per the Confederation of Indian Industry and with the adoption of technology their contribution is only likely to grow. A consulting firm has expected a consumption of $80 billion worth of digital services in next five years but at the same time these businesses lack any strategy to deal with growing threat of cyber security due to lack of resources and manpower. What makes the matter worse is the confidence that they are not at the risk. For building any strategy it is pertinent to do risk assessment. A mind-set inclined towards carelessness in cyber security strategy can be extremely harmful for any company. A July 2019 study by UK based cyber-security firm Keeper Security found that decision makers in 62% of companies between $1 million and $500 million did not think they would be the target of cyber-attacks. It is this perception which may discourage them to spend enough on cyber-security. Lack of knowledge and deficiency of time and budget are three common reasons why businesses may not have adequate cyber security today. Protection with implementation of proper tool can cost a lot to already cash crunched small businesses and the only way out for them would be taking preventive cost effective measures. These could include employee training: this most under rated measure could actually be a very simple and effective answer to cybercrimes. Time to time seminars on safe cyber practices and ways to identify the attacks can save employee and company from becoming a victim of cyber-crime. The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. A research found out that Sixty percent of respondents in companies that had a data breach say the root cause of the data breach was a negligent employee or contractor, an increase from 54 percent in 2017. Sixty-one percent of respondents say negligent employees put their company at risk for a ransomware attack. Another possible way would be installing multifactor authentication. Such a technique can save a company from any attacker who has gained...

24ber-mindset-exposed-keeper-unveils-its-2019-smb-
cyberthreat-study/.
25 How Small Businesses Can Improve Cybersecurity Without Breaking the Bank https://www.securitymagazine.com/articles/91543-
26how-small-businesses-can-improve-cybersecurity-
without-breaking-the-bank.
27 Supra note 21
Username and other credential for logging in and gaining access to sensitive data. Constant upgrade of software and strong password could also be an effective way for SMBs to protect their data. This tedious but effective precautionary measure is a powerful against cyber-attacks and is a successful way to reduce great risk in an economical way. A cyber security company’s research report showed that, “Nearly 7 in 10 respondents (69%) affiliate passwords with security or a first line of defence against an attack. 75% of companies have policies in place that encourage or require employees to update their passwords regularly. Among leaders surveyed, CEOs, Chairs and Owners were more likely to not know company password policies (13%)”.

According to an August 2019 report by Russian cyber-security firm Kaspersky, despite the availability of newer versions of software, around 41% of consumers still use either an unsupported or approaching end of support desktop operating system. About 40% of very small businesses and 48% of SMBs continue to rely on older version operating systems. This highlights another problem whose solutions lies in having up-to-date antivirus software on all company devices and network. Another cost effective solution for SMBs could be using cloud technology saving them from employing high end expensive security within their storage facility to protect data theft. Rather a simple practice of backing up their data with cloud based storage could provide the basic protection.

[4] **Cloud storage: A one stop solution?**

A trend shows professional services and manufacturing companies report a higher usage of cloud applications than other industries. This has to be changed and similar inclusions should be made by most of the companies. A report shows that virtually all of the participant respondents have already deployed cloud applications or plan to deploy them in the next 12 months, the benefits of clouds appear to outweigh the risks to most organizations thereby implying a growth in knowledge about benefits of cloud applications.

Inclusion of cloud storage has blurred the boundaries of company’s infrastructure making it difficult to precisely target an organisation’s resources. At the same time difficulty will also increase for a company to identify targeted attacks at an early stage and separate them from the overall mass of attacks on the ISP. What is alarming is that awareness of cloud infrastructure security is not growing as fast as the popularity of cloud services. For the companies planning to deploy security services in 2020 must note that with shifting of data storage facility, criminals will also migrate to the cloud and will forge ahead, therefore what could save is providers reviewing their security practices.

---

28 Supra note 27  
29 Supra note 25  
31 Supra note 11  
32 Id.  
and infrastructure and establishing a continuous communication with cloud service provider and instant information of report on data breaches in case any attack identification.

[5] WAY FORWARD

Gartner predicts that global security spending will be influenced by an increased focus on building detection and response capabilities, privacy regulations, and the need to address digital business risks in 2019. Worldwide spending on security-related hardware, software, and services is forecasted to reach $133.7 billion by 2022.34

Now the best practice for any company would be to deploy technology which suits their needs rather than sticking to the model deployed by other companies. Also securing of most costly and sensitive date should be primary priority.

Revising the cyber security budget after identifying the strength and weakness of current cyber security strategy should be another required move that would be helpful in allocation of correct budget for company’s needs and for continuous training and education of all employees in order to prevent data leak.

Company may not find this profitable in short term but in long run they are going to pay off. Aligning top leadership and cyber security experts is the key to improving a company’s health while increasing efficiency and response time to data breaches remains another.

BIBLIOGRAPHY

Journals

Conference Papers
- Doe, N.P and Suganya V.. Secure service to prevent data breaches in cloud. in Computer Communication and Informatics (ICCCI), 2014 International Conference 2014. IEEE.

34 Supra note 22.
Websites


- Xie Ken, June 2, 2020, we must rethink and repurpose cybersecurity for the covid-19 era https://europeansting.com/2020/06/02/we-must-rethink-and-repurpose-cybersecurity-for-the-covid-19-era/.


- Cybersecurity threats to cost organizations in Asia Pacific US$1.75 trillion in economic losses, (May 18, 2018), https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-


*****