CyberPeace Foundation | Autobot Infosec | UN Global Compact Network India | IETE India

CYBERSECURITY FOR SMEs AND STARTUPS

CYBERSECURITY FOR SMEs AND STARTUPS

TABLE OF CONTENTS

CHAPTERS

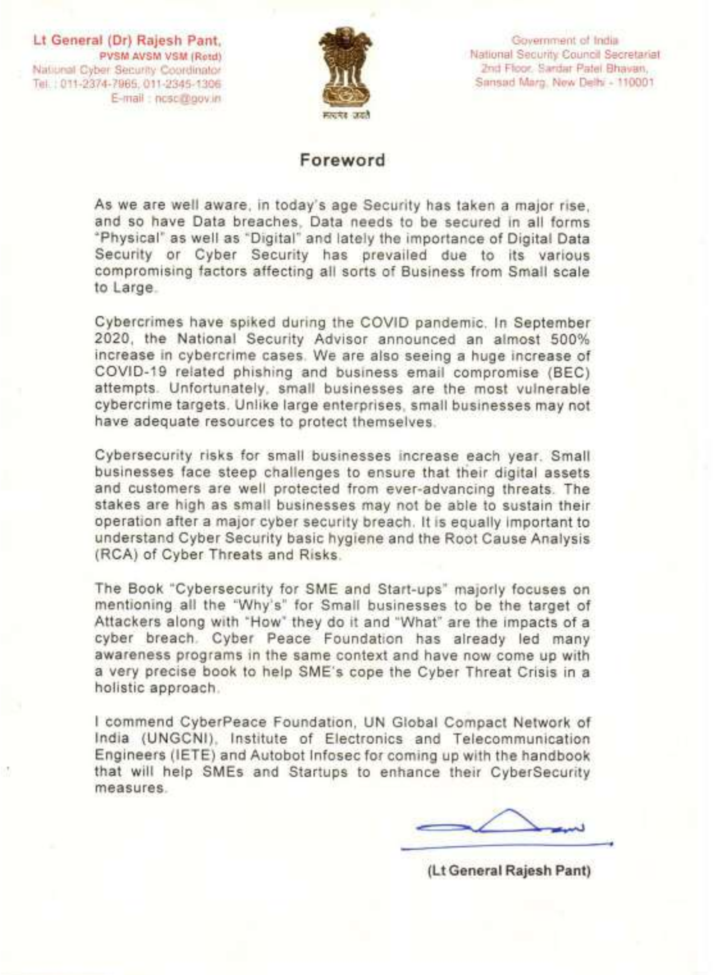
PREFACE

Digital transformation has changed the way individuals behave, and businesses operate. Alongside, cybercrime has also made its presence felt across all industry domains. The cybersecurity market today is at its prime in 2020, but this hasn't always been the case. Back in the 80s and 90s, cybersecurity wasn't such a critical topic and an integral factor responsible for an organization's well-being as its today. But over the years, terms like ransomware, malware, trojan, etc., have terrorized the internet in such a way that people seldom deter from making investments in cybersecurity and learning more about the subject.

With the idea of propagating cybersecurity knowledge, education, and training to every employee in an organization, especially SMEs (Small and Mid-sized Enterprises) and startups, here is a book with a wide range of topics covering right from the most basic controls to highly sophisticated security measures enterprises can adopt.

The book shall be especially beneficial in understanding cybersecurity basic hygiene, education and prove to be a handy asset to cybercrime investigators, security specialists, security consultants, IT experts, etc. This book extensively discusses the Root Cause Analysis (RCA) of cyber threats & risks, zero day vulnerabilities, threat management, protection from phishing, and other security risks facing organizations today.

FOREWORD



Lt General (Dr) Rajesh Pant,
PVSM AVSM VSM (Retd)
National Cyber Security Coordinator
Tel. : 011-2374-7965, 011-2345-1306
E-mail : ncsc@gov.in

सत्यमेव जयते

Government of India
National Security Council Secretariat
2nd Floor, Sardar Patel Bhavan,
Sansad Marg, New Delhi - 110001

Foreword

As we are well aware, in today's age Security has taken a major rise, and so have Data breaches, Data needs to be secured in all forms "Physical" as well as "Digital" and lately the importance of Digital Data Security or Cyber Security has prevailed due to its various compromising factors affecting all sorts of Business from Small scale to Large.

Cybercrimes have spiked during the COVID pandemic. In September 2020, the National Security Advisor announced an almost 500% increase in cybercrime cases. We are also seeing a huge increase of COVID-19 related phishing and business email compromise (BEC) attempts. Unfortunately, small businesses are the most vulnerable cybercrime targets. Unlike large enterprises, small businesses may not have adequate resources to protect themselves.

Cybersecurity risks for small businesses increase each year. Small businesses face steep challenges to ensure that their digital assets and customers are well protected from ever-advancing threats. The stakes are high as small businesses may not be able to sustain their operation after a major cyber security breach. It is equally important to understand Cyber Security basic hygiene and the Root Cause Analysis (RCA) of Cyber Threats and Risks.

The Book "Cybersecurity for SME and Start-ups" majorly focuses on mentioning all the "Why's" for Small businesses to be the target of Attackers along with "How" they do it and "What" are the impacts of a cyber breach. Cyber Peace Foundation has already led many awareness programs in the same context and have now come up with a very precise book to help SME's cope the Cyber Threat Crisis in a holistic approach.

I commend CyberPeace Foundation, UN Global Compact Network of India (UNGCNI), Institute of Electronics and Telecommunication Engineers (IETE) and Autobot Infosec for coming up with the handbook that will help SMEs and Startups to enhance their CyberSecurity measures.

(Lt General Rajesh Pant)

FOREWORD

Prof. (Dr) J W Bakal
M.Tech., Ph.D.
President

The Institution of Electronics and Telecommunication Engineers (India)
#2, Institutional Area, Lodi Road, New Delhi - 110 003
Tel. : 011-43538821 (O)
Fax : 011-24649429
Mobile : +91 9594962007
E-mail : president@iete.org
bakaljw@gmail.com
Vebsite: www.iete.org

Message

It gives me immense pleasure to know that IETE Ranchi Centre, in association with Cyber Peace Foundation, is organizing a Webinar onCyber Security for SMEs and Start-ups on 22nd Oct 2020. IETE Ranchi centre's contribution has always been commendable towards the perpetuation of the goals of the Institution.The centre is committed to take ahead the charter of the IETE by serving Student, Corporate & ISF Members in East Zone.

Cyber Security has always been a prime Challenge for organizations, however, during the present COVID times; the challenge has grown even more radical especially for SMEs and Start-ups. SMEs are also faced with a new reality where employees are working more from home. This way they become even more dependent on Information Technology (IT) than before. Small and medium-sized enterprises (SMEs) are often coping with difficult times. Smaller businesses are more likely to be the victims of attacks which can often be disguised as standard business emails. Since they are usually less well protected and easier to compromise, it's easier for cybercriminals to find ways into their networks and even use them as a gateway to larger companies and organisations.

Smaller companies play a key role in a country's business community so it is important that they remain a focus when it comes to developing solutions and policies to help them effectively manage this risk.To address this pervasive problem, governments around the world need to fundamentally realign their cyber Security efforts.

I am confident that with several eminentexperts andinvited speakers, the Webinar will be a grand success. I also believe the deliberations on the selected theme will enlighten us with effective ideas and solutions to overcome the obstacles so that even the smallest of companies do not fall prey to the cyber-attackers.

Prof (Dr) J W Bakal

FOREWORD

Network India

Global Compact Network
UNESCO House, 1st Floor
1, San Martin Marg, Chanakyapuri,
New Delhi - 110021
Phone : +91-11-2611 1071/72
Email : gcnindia@globalcompact.in
Web : www.globalcompact.in

Companies from different sizes and in different sectors are increasingly relying on Information and Communication Technologies, and this has been key to innovation, productivity and growth. Despite the countless benefits and opportunities, there are challenges that arise in the Cyber Space, and small and medium enterprises (SMEs), generally face higher challenges if compared to larger companies. Having a poor infrastructure, not knowing how to properly address complex cybersecurity threats, or underestimating the importance of protecting personal data are examples of these challenges faced by SMEs.

Cyber threats are a significant business risk for SMEs. With practices increasingly moving towards the Internet and cloud, SMEs have a larger attack surface than ever before. According to the NCSC (National Cyber Security Centre), SMEs have a 1 in 2 chance of experiencing a cyber breach. The Ponemon Institute reports that the average cost of a data breach for organisations with up to 500 employees is $2.17m. As SMEs work to protect themselves in an ever-evolving threat landscape, they find their security needs are constantly changing.

This Book therefore briefly describes some of the difficulties faced by SMEs given the increased Cyber Threats. It also addresses crucial considerations pertaining to data protection and privacy, and the importance of making some changes that allow for a "security-aware" culture to be created. It also explains how SMEs can enable a healthy ecosystem, such as the adoption of cybersecurity standards. Lastly, a few straightforward steps that can be taken by SMEs when looking at strengthening their cybersecurity preparedness which are outlined.

I would like to congratulate Mr. Vineet Kumar and his team for materializing this wonderful concept and cyber securing SME's and Startups in this era of Online World.

Kamal Singh
Executive Director
UN Global Compact Network India

FROM THE PRESIDENT'S DESK

The World Economic Forum regards the threats to cybersecurity as one of the top five global risks facing the world today. The vulnerabilities of financial loss ranging from cybersecurity breaches to theft of intellectual property are a growing problem. At the same time, potential for cyber-attacks to disrupt critical services of both private enterprises and government agencies is growing at an alarming rate. These transformational challenges are also occurring as a result of increase in digitization of services, social media, internet of things, increased automation, cloud computing, big data and related applications. The potential impact that these transformational changes will have on the field of cybersecurity will be enormous and will create a need for continuous trainings.

The costs and ways of implementing cybersecurity in organizations has been a constant burden on any leadership regardless of their size, area of operations etc. Through this initiative, we have tried to elucidate some of the proven-effective and cost-efficient cybersecurity integration methods for small to medium scale industries.

This book addresses some pertinent issues and vulnerabilities that organizations might face such as ransomware, zero-day attacks, DDoS etc. This book is positioned to serve as a guide for medium and small-scale businesses to strengthen their cybersecurity capabilities while securing their networks and human resources. Apart from technical aspects of security, the book also builds awareness about incident response, attack recovery plans that many organizations often struggle with.

I commend and thank everyone because of whom this concept and book has been made a realistic dream.

Vineet

Vineet Kumar
Founder and President

INTRODUCTION

This book focuses on cybersecurity for SMEs and Startups. It entails a detailed study of the trends of cyberattacks on Small and Medium Enterprises and startups. The book first mentions the most common cyber threats attacking SMEs and then stresses the dire need for cybersecurity solutions, tools, and frameworks in an organization. It gives an insight into the various security options available in the market today to protect company networks.

The book discusses how cyber adversaries exploit security vulnerabilities, but also cyber threats, and provides practical suggestions, mitigation measures, and best practices that may be employed to harness any investment in cyber-security to the optimum level.

Often we address the problem but fail to address the after-effects of a cyber attack. The book has a section dedicated to discussing cyberattack recovery measures. Disaster recovery plans have been discussed at length to bring about a faster recovery rate among organizations struck with cyberattacks.

Chapter 1

Cybersecurity: A Must For SMEs And Startups

The adage "Hope for the best, but be prepared for the worst." has tremendous significance in today's digital world. Every business organization is dependent on computers and the internet for their functioning and hence prone to cyberattacks from malicious actors. The only solution to manage cyber risks is to have a robust cybersecurity strategy and framework in place that can prevent the attacks and can withstand in the aftermath of an attack, if at all, it happens. Though large corporates and institutions are at perennial risk, SMEs (Small and Medium-sized Enterprises) and startups can also not afford to ignore cyber threats.

1.1 Why Do Cybercriminals Target Small Organizations?

There is a general preconception among SMEs and their thinking is like, "Why would cyber criminals attack my business when there are enormous targets available in the industry." However, the reality couldn't be farther than this.

SMEs and small businesses are incredibly vulnerable to cyberattacks due to the following reasons.

- Compared to corporate institutions, small business enterprises cannot afford to install the highest security measures. The absence of security guards, sophisticated monitoring systems, and technically equipped entry devices tempt cybercriminals as they can attack without fearing detection.

- Secondly, all cybercriminals may not have enough motivation to break into the high-security networks of large corporates. Vulnerable SMEs and startups are easier targets.

- Small businesses overlook the value of data they store by believing that it can be of little importance. However, there is a lucrative market for such data on the dark web.

- Usually, targeting SMEs can pave a smooth passage for malicious actors to hack into the corporate network because these SMEs are critical links to many corporate supply chain networks.

- Cybercriminals find it convenient to use tactics like spear-phishing against SMEs. It also enables them to enter corporate networks as legitimate users.

1.2 Ignoring Cybersecurity Can Prove To Be Fatal

In today's world of online business, any laxity in cybersecurity can have dangerous consequences. It can lead to financial loss, mistrust among customers, and damage the business' reputation in the market.

1.2.1 Recent Statistics On Cyberattacks

The recent statistics on cyberattacks on small businesses and SMEs can be startling.

- Of all cyberattacks, 43% target small businesses and SME startups (1).

- Nearly 47% of SMEs have no clue about managing cyber risks (2).

- About 60% of such small enterprises that turn victims of cybercrime go out of business within six months (3).

- 91% of small business entities do not have cyber liability insurance (4).

- Yahoo has been the victim of the most significant cyberattack when more than three billion accounts were compromised in August 2013 (5).

1.2.2. Examples Of Cyberattacks Against Startups

Here are a couple of examples of cyberattacks against startups that should put SMEs on their guard (6).

- Efficient Services Escrow Group, a California financial organization, had to shut down its business after cybercriminals siphoned off more than $1.5 million from the company's bank account using a Trojan Horse software. After breaking into the system, the malicious actors transferred the amount to different accounts in Moscow and China. The organization managed to recover $0.43 million but lost almost $1.1 million, forcing the state regulators to close down the firm.

- In Kansas, an automobile dealership enterprise, Green Ford Sales, lost nearly $23,000 as malicious actors broke into their system and swiped bank account information. The criminals opened nine fictitious employee accounts and added them to the payroll.

Subsequently, they transferred $63,000 to these nine accounts. The organization managed to recover nearly $40,000 of the stolen money.

1.3 How Improving Cybersecurity Provides Competitive Advantages

Compromising on cybersecurity aspects jeopardizing customer data can prove detrimental to the overall success of an enterprise. Here's how improving cybersecurity provides a competitive advantage to SMEs and small businesses.

- Higher customer preference - Customer surveys show that consumers prefer dealing with businesses that concentrate on data privacy and cybersecurity. Such aspects rank ahead of the pricing aspect, proving to be one of the top reasons for them to do business with a specific retailer.

- Greater customer satisfaction – Customer satisfaction is higher when the business entity focuses on implementing cybersecurity and data privacy capabilities. Customers value robust cybersecurity postures like encryption of data, offering transaction alerts and prompts for account passwords, and so on.

- Higher spending online – Business apps that concentrate on building trust by using advanced security techniques like TLS or SSL witness a higher volume of customer traffic. Surveys show that nearly 40% of customers are willing to enhance their online spending by 20% if retailers offer trust-building assurances.

Source - Capgemini

In A nutshell

A global increase in cyberattacks on business organizations has forced SMEs to concentrate on implementing robust cybersecurity strategies in recent times. Staying prepared for the worst can undoubtedly help these businesses to manage cyber risks better. Cybersecurity is a must for all business organizations, notably the SMEs and startup enterprises.

References

1. Technology Trends, Joshua Sophy, 43 Percent of Cyberattacks Target Small Business, https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html

2. Keeper Security, Ponemon Institute LLC, 2018 State of Cybersecurity in Small & Medium Size Businesses, https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

3. The Denver Post, Garry Miller, 60% of small companies that suffer a cyberattack are out of business within six months https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/.

4. Insurance Bee, Cybercrime survey reveals SMB owners are unaware and unprepared, https://www.insurancebee.com/blog/smb-owners-unprepared-for-cybercrime.

5. CPO Magazine, Matt Powell, 11 Eye Opening Cyber Security Statistics for 2019, https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/

6. Syscon, Stories from Small Businesses that were Attacked, https://syscon-inc.com/stories-from-small-businesses-that-were-attacked/

Chapter 2

The Biggest Cybersecurity Risk Facing Organizations Today

When it comes to the most common challenges faced by organizations, one of the most critical ones is the cybersecurity risks. They interrupt the functioning of an organization and compromise the confidentiality, integrity, and availability (CIA) of valuable information assets. However, the cybersecurity risks themselves stretch across a broad spectrum. Let's have a look at the most critical cybersecurity risks organizations face today.

2.1 Negligence By Employees

A lot of money is invested by the organizations to train the personnel on various cybersecurity threats. Despite it, the sensitive data of the organization gets compromised repeatedly. The primary reason for this is the negligence of employees. A significant cause of security breaches is human errors, as published in a recent report by IT security firm Shred-it. The employee habits that lead to data breaches include:

- Accidentally losing the document or mobile device that contains confidential data or passwords
- Leaving the workstation unlocked or unattended.
- Noting essential information on loose paper notes and leaving them out on the desk.
- Remote working using an unsecured, public network connection

Appropriate steps, such as the following, are essential taken to solve the issue:

- Creation of a robust cybersecurity policy
- Conducting regular training sessions
- Creation of a clean desk policy (CDP)
- Disposal of hard-drives and flash drive in the proper manner
- Creation of an appropriate remote access policy

2.2. Lack Of Adequate Protection

An increase in the number of incidents relating to cybersecurity data breaches has made organizations concerned about the adequacy of cybersecurity measures. Most organizations ignore cybersecurity due to the high-investment requirement, which results in a lack of adequate protection to prevent cybersecurity threats. Such ignorance could incur a massive expense to the organization in the form of a data breach.

The usual anti-virus software or firewall alone is not sufficient to combat cyber-attacks. For the protection of confidential and sensitive data, any computing environment needs:

- An updated cybersecurity policy.
- Continuous training of employees.
- Multi-factor authentication.
- Insurance for cyber liability.
- Anti-malware software.
- Security measures for the use of IoT devices

2.3 Employee Mobility

Employee mobility is the latest trend that organizations are following to increase productivity. A reduction in commuting time and flexibility in work hours has helped employees to work more efficiently. However, there are certain risks too, which include an increase in the vulnerability to cyberattacks.

Employee mobility presents organizations with a bunch of alarming challenges:

- While working remotely, employees mostly use personal devices that are less protected,
which results in a data breach.
- Usage of the unsecured public network can cause malicious actors to break into the devices.
- IoT devices used by telecommuting employees have a direct connection with the organization's server. A minor breach in the device can compromise the whole data present on the server. The Russian-state sponsored attack, Fancy Bear, is one of the best examples of network vulnerability.

To manage the security issues of employee mobility, organizations need to:

- Initiate an awareness drive to ensure that employees stick to security protocols.
- Create a secure enterprise app that can support most of the IoT devices.
- Issue the organization's devices to employees to prevent BYOD **(Bring Your Own Device)** issues.
- Conduct seminars and training sessions to educate employees on potential risks.

2.4 Absence Of A Functioning Data Backup Policy

Backing up the organizational data is one of the essential activities contributing to cybersecurity. In case of any network exposure or loss of data due to a disaster, backed-up data enables the organization's continual operations without interruption. Negligence with data backup can leave the organizational data vulnerable to a variety of cybersecurity threats.

The organizations should:

- Create a security policy for data backup.
- Create a rigorous awareness campaign among the employees to convey the importance of data backup.
- Backup data regularly.

2.5 Poorly Defined Cybersecurity Policies

Cybercriminals attack organizations from every industry. It is high time organizations prioritized cybersecurity policy and security standards to strengthen its cybersecurity framework and data protection posture.

The cybersecurity policy must include:

- Identification of cybersecurity risks.
- Establishment of cybersecurity governance.
- Creation of policies, procedures, and processes for protection of the organization's networks and information assets
- Identification and reporting of risks related to remote access and fund transfer
- Identification and handling of risks concerning vendors including third parties
- Strategy to detect unauthorized and malicious activities

Final Words

Cybercriminals have become more robust and use advanced and sophisticated techniques to attack organizations. The most significant cybersecurity risks happen with negligence in smaller matters. Hence, it is essential to evaluate the organizations' cybersecurity risks and develop an efficient cybersecurity strategy accordingly. It goes a long way in protecting the organization as far as the confidentiality, integrity, and availability of its valuable information assets are concerned.

References

1. Insuretrust, Employees and Cybersecurity Risks–Why Negligence Is the Biggest Threat, https://www.insuretrust.com/employees-and-cybersecurity-risks-why-negligence-is-the-biggest-threat/

2. CNBC, Carmen Reinicke, The biggest cybersecurity risk to US businesses is employee negligence, study says, https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html

3. HighlandRisk, Here Are the Reasons Why Many Organizations Don't Have Proper Cybersecurity Measures in Place, https://www.highlandrisk.com/here-are-the-reasons-why-many-organizations-dont-have-proper-cybersecurity-measures-in-place/

4. Noah Gamer, Mitigating the cyber risks of enterprise mobility and BYOD, https://blog.trendmicro.com/mitigating-the-cyber-risks-of-enterprise-mobility-and-byod/

5. Entrepreneur India, Remesh Ramachandran, Enterprise Mobility And Role Of Strict IT Security Policies In Improving Workplace Mobility In An Organization, https://www.entrepreneur.com/article/346926

6. Crowd Strike, Who is FANCY BEAR (APT28)?, https://www.crowdstrike.com/blog/who-is-fancy-bear/

7. ITProPortal, Rod Mathews, Avoiding the biggest threats to data backup, https://www.itproportal.com/features/avoiding-the-biggest-threats-to-data-backup/

8. CCSI, Larry Bianculli, 10 Common IT Security Risks in the Workplace, https://www.ccsinet.com/blog/common-security-risks-workplace/

Chapter 3

Most Common Cyberattacks Targeting SMEs and Startups: What You Must Know!

Cybersecurity is of paramount importance for all business entities, notably the SMEs and startup enterprises, to safeguard the confidentiality, integrity, and availability of their valuable information assets. In this episode, we shall discuss the different types of cybercrimes that malicious actors deploy to target SMEs and startup entities. Simultaneously, let's examine specific feasible solutions too.

3.1 Ransomware

Ransomware (1) is gaining notoriety for being the most preferred cyberattack on SMEs and startup business enterprises in recent times. Cybercriminals usually introduce ransomware through a phishing email attachment, masquerading as communication that businesses trust to be genuine. Once opened and downloaded, the malware takes over the victim's network system and corrupts the files and documents. The cyber attacker then demands the payment of a ransom to restore access to the network.

The Solution - The solution to ransomware is to ensure not to open unsolicited emails or download suspicious attachments. Having a dedicated backup on an isolated network system can help the business ignore the ransom demand and restore it.

3.2 Cryptojacking

Using someone else's computer system in an unauthorized way to mine cryptocurrency is referred to as Cryptojacking. Nowadays, cryptocurrency is in high demand globally. Today, it is becoming increasingly challenging to mine cryptocurrency. Cryptojacking (2) criminals access the network systems of SMEs and other businesses unauthorizedly to mine cryptocurrency.

The Solution – Installing a robust internet security software solution can block most of the cryptojacking threats. But employee training on cybersecurity also plays a critical part.

3.3 Phishing

Phishing (3) is one of the oldest and most common cybercrimes present in the industry. Here, the malicious actor contacts the targets through emails, text messages, or telephone by posing as a legitimate entity that the target trusts. The objective is to lure the target SME to part with sensitive information regarding the business or its customers. The data can include trade secrets, banking account information, and customer data.

The Solution – Increasing awareness among IT users to not open emails from unknown sources and suspicious contacts can help businesses manage phishing attacks. Installing anti-phishing software can minimize such attacks.

3.4 APT Attacks

APT (Advanced Persistent Threat) (4) is an attack where the cybercriminal establishes a long-term illegal presence on the SME/business entity's network to access sensitive data. The motive is to steal intellectual property, compromise confidential information, sabotaging critical organizational infrastructure, and so on.

The Solution – Protecting against APT requires businesses to adopt a multi-faceted approach that includes monitoring web traffic, whitelisting domains, and applications, controlling access, and patching network software.

3.5 Insider Based Attacks

Insider threats (5) from disgruntled employees having access to sensitive information can cause more damage than external threats. Such employees can leak out the business's confidential data to competitors or other malicious actors to cause harm to the organization.

The solution – Monitoring the activities of employees is one way to manage this threat. Restricting access to sensitive information to employees can help protect the business from insider threats.

3.6 DDoS

DDoS means Distributed Denial of Service (6). Here, the cybercriminals attempt to disrupt regular internet traffic of a targeted digital network server by overwhelming it with an additional flood of traffic. Consequently, the usual traffic gets delayed or interrupted.

The solution – The ideal solution could be to create a blackhole route and direct traffic to that route. Other solutions include rate limiting, installing web application firewalls, and using an Anycast Network.

3.7 Man in the Middle Attacks (MitM)

Man in the Middle Attack (7) is an intercepting attack by a third person unknown to the target. Such criminals intercept business communications to steal critical information. A simple example of a MitM attack is where the malicious actor sends a phishing email to the target. The email appears to generate from a legitimate source such as the bank. On clicking the link, it directs the target to a fake website resembling the bank site, whereby they enter the login credentials and make it convenient for the MitM to access the bank accounts.

The solution – Businesses should ensure that the URL has HTTPS instead of HTTP. Employees should also be taught and trained not to connect to public WiFi routers. Securing the office and home networks can also help ward off MitM attacks.

3.8 Password Targeting Attacks

Password thefts or stolen credentials account for nearly 29% of data breaches (8). Therefore, having a strong password is imperative for avoiding such attacks. Cybercriminals prey on targets by using various types of password attacks (9), such as the following.

- **Brute Force attack –** using brute force by using all password combinations.
- **Dictionary attack –** trying out different possibilities of passwords that the target extensively uses.
- **Phishing –** sending unsuspected emails
- **Rainbow Table attack –** a sophisticated type of a brute force attack
- **Credential stuffing –** random use of stolen usernames and password combinations
- **Password spraying –** using a list of commonly used passwords.
- **Keylogger attack –** surreptitiously using software to record keystrokes of the target.

The solution – The ideal solution is to use a strong password that becomes impossible to guess. The most secure password should be a combination of capital and small letters of the alphabet, special characters, and numeral. Another solution is to use alternative verification methods such as 2FA and biometric authentication as supplementary controls.

3.9 SQL Injection Attacks

SQL Injection attacks (10) are sophisticated cyberattacks where the cyber adversary takes advantage of SQL Injection vulnerabilities for bypassing application security measures. This attack enables the cybercriminal to execute malicious statements to control a database server behind a web application.

The solution – The only way to overcome an SQL injection attack is input validation and parameterized queries. Sanitizing all inputs, including login forms and removing malicious code elements, can help prevent SQL injection attacks. The simple answer is strong application security policy, processes, and guidelines.

3.10 Zero-day Attacks

A zero-day attack (11) is a flaw or a vulnerability in the software or hardware that can create complications if exploited by the cybercriminal.

The solution – The only way to manage a zero-day attack is to address the issue before someone exploits the vulnerability. Hence, software developers release patch programs to fix the vulnerability.

Final Words

Cybercriminals are a resourceful lot. They are always on the prowl to pounce on any vulnerability in the network systems. We have seen ten different ways these malicious actors gain access to network systems and compromise with sensitive information. The best ways to manage these crimes are to be vigilant, employ safe practices when using the internet, and know the vulnerabilities. Installing high-quality anti-malware solutions can help mitigate such threats. SMEs and small businesses should have a robust cybersecurity strategy to manage such cyber risks and protect data from being misused by these criminals.

References

1. CSO, Josh Fruhlinger, Ransomware explained: How it works and how to remove it. https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

2. Norton, What is crypto-jacking? How it works, how to help prevent it. https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html#:~:text=Cryptojacking%20is%20the%20unauthorized%20use,cybercriminals%20to%20mine%20for%20cryptocurrency.

3. Phishing.org, What is Phishing? https://www.phishing.org/what-is-phishing

4. Imperva, Advanced Persistent Threat, https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

5. CSO, Dan Swinhoe, What is an insider threat? Seven warning signs to watch for, https://www.csoonline.com/article/3323402/what-is-an-insider-threat-7-warning-signs-to-watch-for.html#:~:text=Insider%20threats%20can%20take%20the,to%20wants%20revenge%20or%20money.

6. Cloudflare, What is a DDoS Attack? https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

7. Norton, What is a man-in-the-middle attack? https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

8. Verizon, 2019 Data-Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

9. Lifars, Types of Password Attacks, https://lifars.com/2020/04/types-of-password-attacks/

10. Acunetix, What is SQL Injection (SQLi), and How to Prevent It? https://www.acunetix.com/websitesecurity/sql-injection/

11. FireEye, What is a zero-day exploit? https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Chapter – 4

How Can SMEs And Startups Secure Their Networks?

We always hear of information network security breaches in the news, and know that they cost enterprises millions of dollars. As per a report by IBM, the average cost to a US enterprise from an incident was $8.1 million in 2019. There must be a lot on the entrepreneur's mind when deciding to start a new business like information flow, finance, marketing, production methods, etc. In the rushed up situation of setting up a business, the security aspect usually gets neglected, which invites malicious intrusions in the enterprise network, jeopardizing the confidentiality, integrity, and availability of the organization's information assets. Hence, the cybersecurity aspect is as crucial as others. The following are the ways how startups and SMEs can protect their networks From malicious actors.

4.1 Use A Powerful & Trusted Antivirus Software

Malware is an old threat and has been around since the early 1980s. And an antivirus program is one of the oldest techniques to thwart malware threats. Antivirus and anti-malware programs can block the execution of any malicious program once they detect it. Hence, as a critical control measure, all businesses, big and small, must install a robust antivirus program in their client workstations.
One has to make note that:

- All Windows PCs must run an antivirus.
- It is a myth that MacBooks do not require an antivirus. They are as vulnerable as Windows systems.
- App-only platforms have different case-use when it comes to antiviruses.
- Installing a strong antivirus solution is not enough. Enterprises must ensure that they have processes in place to update the antivirus signature database regularly.

4.2 Configure Firewalls Properly

As a general rule, firewalls are crucial for protecting the networks in businesses of all sizes. SMEs and startups must install efficient firewalls on all their devices and set up a web application firewall (WAF). It becomes even more critical for e-Commerce platforms that sell their products online. They store the confidential customer data which needs protection from malicious access.

4.3 Backup Data Regularly To Protect Against Breaches

It is a common practice for organizations to back up their crucial data in Cloud drives like OneDrive and Google Drive. However, as these drives are online, they are as vulnerable as the internal system's storage itself when the malicious actors gain unauthorized access to valuable information assets. They can modify and encrypt data as quickly as the owners themselves. Hence, business owners should keep offline backups of their crucial enterprise data.

4.3.1 The 3-2-1 Rule Of Backup

The 3-2-1 Rule is another essential and useful safeguard an enterprise must diligently follow to defend its valuable information assets. It is described as below.

- **Keeping At Least Three Copies Of The Data**
  One backup doesn't cut it if enterprises store it on the same premise as primary data. The higher the number of copies, the lesser the chances of exposing them to a threat, all at once.

- **Storing Two Backups On Different Storage Media Or Devices**
  Two similar devices have a higher risk of exposure than two different devices with variable storage media.

- **Keeping At Least One Backup Copy Offsite**
  Keeping at least one copy offsite is a safeguard against disasters that may damage all copies of data stored in one place.

4.3.2 Choosing the right data centre

If one's organization has an online presence and holds a lot of customer data, which is Sensitive, such as an e-commerce platform, a social media platform or an offline mart that collects customer data for loyalty programs, choosing a correct data centre, to store all that data, can be a very important decision. There are several types of data centres which offer a different kind of services such as variations in data redundancies and backups, power backups, maximum downtime etc.

These data centres offer downtime ranging from 99.5% to 99.99%, while the decimal difference doesn't look huge on paper, the actual difference of these ranges is usually in days. Complying with laws on data localization and cross border data transfer also becomes an important factor when deciding a data centre. Therefore, such a decision of selecting a Data Centre must be done after thorough market research and professional advice.

4.4 Encrypt Everything To Protect Sensitive Data

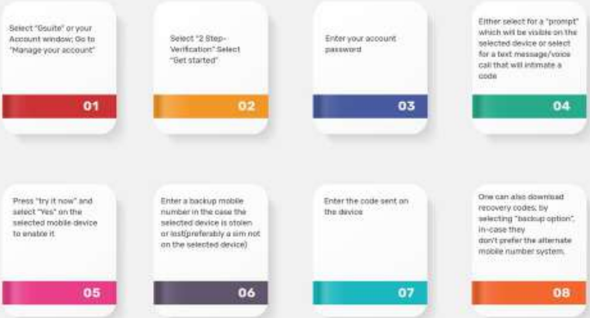
SMEs must protect sensitive information transferred over the internet through encryption. Encryption is the process of changing the data into a virtually unreadable form, retrievable only with a decryption key. End-to-end encryption is a powerful security mechanism as no unauthorized user can access the information without the decryption key.

4.5 Use Two-Step Authentication And Password Security Software

Two-factor authentication (2-FA) is a process that further enhances the security of the network. In 2-FA, if the server notices a new device login attempt, it will ask for additional authentication through a different channel, like a text message on the user's cell phone. Responses to such text messages prove that users themselves possess their cell phones. Thus, 2-FA acts as a barrier to phishing since a malicious actor cannot log in by merely knowing a user's password.

4.6 Enabling 2 factor authentication on your Email

Here's how one can enable it on Gmail or GSuite account.



Select "Gsuite" or your Account window; Go to "Manage your account" 01

Select "2 Step-Verification" Select "Get started" 02

Enter your account password 03

Either select for a "prompt" which will be visible on the selected device or select for a text message/voice call that will intimate a code 04

Press "try it now" and select "Yes" on the selected mobile device to enable it 05

Enter a backup mobile number in the case the selected device is stolen or lost(preferably a sim not on the selected device) 06

Enter the code sent on the device 07

One can also download recovery codes; by selecting "backup option", in-case they don't prefer the alternate mobile number system. 08

4.7 Update All Software Regularly

Usually, as enterprises become more aware of the threat landscape, they invest in security programs. However, they must note that purchasing and installing is just the beginning. They must update these programs regularly to deter all threats to the information network.

Final Words

Setting up an efficient security program for their fledgling enterprise is a prerogative of new business owners. They can talk to a professional who can help them develop a comprehensive approach fitting their budget. Assessing the network and usage is a crucial step to ascertain if the setup requires any safety upgrades. Although it may seem burdensome, it can protect the essential information resources when the organization faces a threat.

SAFE SERVER

ANTIVIRUS

NETWORK SAFETY

FINGERPRINT LOCK

References:

1. *Crispin Cowan, 2017, Top 6 Ways to Protect Your Startup From Cyber Attacks, https://www.liveplan.com/blog/top-6-ways-to-protect-your-startup-from-cyber-attacks/*

2. *Sam Bocetta, E-C Council, 8 Steps For Startups To Secure Their Network Against Threats Before 2020, https://blog.eccouncil.org/8-steps-for-startups-to-secure-their-network-against-threats-before-2020/*

3. *Chelsea Segal, CoxBLUE, Network Security Best Practices – A 12 Step Guide to Network Security for Business, https://www.coxblue.com/how-to-secure-your-business-network-a-12-step-guide-to-network-security/*

4. *Alex Mayer, 2017, The 3-2-1 Backup Rule, https://www.nakivo.com/blog/3-2-1-backup-rule-efficient-data-protection-strategy/*

5. *Oracle9i Security Overview, Protecting Data in a Network Environment, https://docs.oracle.com/cd/B10501_01/network.920/a96582/protnet.htm*

Chapter 5

Cybersecurity Best Practices For SMEs And Startups

SMEs and startup entities usually think that cybercriminals will bypass attacking their organizations because there is not much to steal. No target is small or big for cyber adversaries. It is up to the business entities to follow adequate safeguards and enforce the best cybersecurity best practices to prevent cyber attacks that can tamper with the confidentiality, integrity, and availability of valuable information assets of the enterprise.

5.1 Enforce Safe Practices For Passwords

The Verizon Data Breach Investigation Report 2020 (1) states that 80% of data breaches involve brute force or stolen credentials. Hence, it becomes imperative for small businesses to enforce safe practices for passwords. A secure password is a combination of lowercase and uppercase letters, numerals, and special characters. Changing the password at frequent intervals should also be compulsory for everyone.

5.2 Email Security Best Practices

Phishing is one of the most common malicious practices employed by cyber adversaries to intrude into digital network systems. Malicious actors send infected files and documents through emails. Unsuspecting users download these files, compromising the valuable information assets of the organization. SMEs and startups should install advanced email protection solutions to identify suspicious email traffic that evades policy and traditional signature-based defenses.

5.3 Online Safety Best Practices

Installing firewalls and anti-phishing software are the first lines of defense against a cyberattack. Every SME or startup entity should necessarily install such firewalls to prevent cybercriminals from breaking into their information systems. Multifactor authentication is another excellent online safety practice that a small business computing environment should employ to ward off these cyber threats.

5.4 Offsite Cybersecurity Best Practices

With many people working from home and other off-site locations, it has become necessary for small businesses to observe the best off-site cybersecurity practices like using a VPN (Virtual Private Network) instead of home Wi-Fi and installing robust firewalls on home computers and smartphones. Prioritizing employee privacy is also an essential safeguard against cyber-attacks.

5.5 Document All Cybersecurity Policies

Small businesses usually operate by intuitional knowledge and word of mouth. However, when it concerns cybersecurity practices, it is advisable to document the enterprise protocols as a critical control measure. SMEs can avail of online training facilities offered by the US Small Business Administration Cybersecurity portal (2). One can also take the help of FCCs Cyberplanner 2.0 (3) for preparing the cybersecurity documents and policies.

5.6 Formulate And Practice An Incident Response Plan

Despite adhering to the latest security practices, no one can entirely rule out unforeseen chances for a cyberattack on the business network. Therefore, having an incident response strategy should be foremost on the minds of all business entities. Such a plan helps IT staff detect, respond to, and recover from cyber-attacks and other issues like data loss and service outages.

5.7 Choose Services That Provide Good Customer Support

A small business might not be able to recruit dedicated staff for monitoring cybersecurity issues. Generally, business entities tend to outsource such activities to cybersecurity experts. It is advisable to choose the appropriate cybersecurity service that provides excellent customer support in deterring malicious intrusions.

5.8 Keep Scalability Of Solutions In Mind

Businesses grow with time. The perfect cybersecurity system is one that is capable of covering the complexities of business expansion. SMEs and startups should consider investing in cybersecurity systems and practices that provide easy scalability, thereby catering to business expansion seamlessly.

5.9 Employee Education As The First Line Of Defense

Cybercriminals target the front-line employees to push in their evil attempts. The standard example is that of the phishing emails. Businesses should recognize the fact and make educating employees about the latest cybersecurity practices e a priority.

While a basic awareness about cyber security and threats to the systems should be provided, the manager should be equipped with basic Redressal mechanism or a basic standard of procedure in case there is a data breach or a compromise on the network security. This would include a basic awareness about what kind of cyber-crimes there are, which data of the organization could potentially be compromised, how to contact law enforcement in such scenario etc

5.10 Best Practices For Device Security

In this digital era, the use of the internet is increasing day by day. Businesses use various devices like desktop PCs, smartphones, Wi-Fi routers, and other IoT-enabled appliances for their daily operations. Compromising on the security aspects of even a single terminal can have disastrous consequences.

5.10.1 Computer Systems And Servers

Computers and servers are fundamental links of any business organization network today. The following tips should qualify as the best security practices to ensure the complete security of these devices from cyberattacks.

- Update the software at regular intervals to be in tune with the latest developments in the industry. Upgrading the software is also a healthy practice.
- Remove all unnecessary services to enhance the device's efficiency and stave off any vulnerabilities.
- Use intrusion detection systems to identify and take care of malicious intrusions.
- Hiding server information from prying eyes is essential for all businesses.
- Ensure periodical file and service auditing.
- Ensure regular backup of server information to protect from ransomware attacks.
- Install and maintain security firewalls to prevent malicious actors from trying to gain access.

5.10.2 Mobile Security

Business organizations and customers use smartphones to carry on their business activities through mobile apps and mobile internet. The following tips can help develop a robust mobile security practice.

- Turning on the user authentication feature can help prevent miscreants from misusing your mobile devices.
- One should update the operating systems regularly.
- Avoid using public Wi-Fi for browsing the internet.
- Using a password manager can help remember secure passwords.
- Ensure that mobile devices have remote lock and data wiping features.
- Mobile devices should have an appropriate cloud backup for restoring data quickly.

5.10.3 Wi-Fi Routers And IoT

With small businesses and startup enterprises adopting emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML), there is an increased use of IoT devices and Wi-Fi routers. Securing these devices is of paramount importance.

- Give a specific name to the Wi-Fi router and use a robust encryption method like WPA2 when setting up the Wi-Fi network address.
- Have a separate guest network for people not connected with the business.
- Use strong passwords for accessing Wi-Fi networks.
- Change the default usernames/passwords that come with IoT devices.

- Check the IoT device settings and disable the unnecessary features.
- A two-step authentication feature can help prevent unauthorized access.
- Avoid using public Wi-Fi networks and keep a watch on hardware outages.

5.10.4 Protecting printers and CCTV cameras

A special focus should be given on protecting the security of shared network resources like printers and CCTV cameras. there have been countless attacks by hackers worldwide, attempted on a large scale, on these devices. Such attempts could lead to hampering of important company documents and information or in some extreme circumstances a situation like the Bangladesh Bank Cyber Heist in 2016. Therefore, while implementing network security and setting up encryption infrastructures and devices, special steps should be taken to secure these devices as well.

5.11 Regular audits by professionals

Once the organization is big enough it is just impossible to have any fault that could compromise the data held by the organization. In these scenarios, regular inspections and audits performed by professionals can be very helpful in identifying the potential threats and weak spots of an organization's network and data arrays. It helps in risk management and becomes a factor in business planning as well. "

Final Words

With more businesses functioning online, it has become necessary for all industries, including SMEs and startup entities, to ramp up their cybersecurity efforts. Cyberattacks can target any digital information network at any time in unexpected ways. Therefore, it is always beneficial to be prepared to take on any risk and handle it efficiently. The best cybersecurity practices listed in this chater can help SMEs and startup enterprises protect their data from malicious actors and maintain a safe and secure information sharing environment.

References

1. Verizon, 2020Data Breach Investigation Report, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

2. SBA, Stay safe from cybersecurity threats, https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

3. Federal Communications Commission, Cyberplanner, https://www.fcc.gov/cyberplanner

4. https://www.bbc.com/news/technology-46552339

5. https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

Chapter – 6

How to Select the Right Security Solution?

The cybersecurity threat landscape is growing by the day, and there is a slew of solutions, which are available for the same. However, when it comes to zeroing down on the right security solution, it becomes as cumbersome for organizations as the variety of threats out there. Thus, for selecting the right solution or service, SMEs and startups need to consider several factors. Some of them are as follows.

6.1 Evaluate & Understand the Situations

Cybersecurity risk assessment helps businesses understand, manage, control, and mitigate cyber risks. Thus, it is a crucial factor for optimum data protection efforts.

1. Determine information value

Small businesses do not have the kind of resources larger companies have, which they can use for information risk management. Thus, it is prudent for them to limit the security scope to the most business-critical assets. They must define a standard that will help them to determine the importance of an asset. They can then classify these assets as minor, major, or critical.

2. Identify threats

Any vulnerability that hackers can exploit to breach the organizational security for harming or stealing crucial data is a threat. Apart from hackers, malware, and IT security risks, other security threats include:

1. Natural disasters: Natural calamities like floods, lightning, earthquakes, and fire pose as high a threat as any other hacker.

2. System failure: SMEs need to determine if their systems are running on high-quality equipment. Sub-standard hardware increases the risk of falling victim to attacks.

3. Human error: Educating the workforce about malware, social engineering, and phishing attacks go a long way in protecting the organization's critical information resources.

4. Adversarial threats:

These threat vectors include trusted and privileged insiders, third party vendors, ad hoc groups, nation-states, corporate espionage, etc.

3. Identify Vulnerabilities

A threat exploits a vulnerability to breach the organizational security, steal sensitive information, and harm the organization. Vulnerability analysis, vendor data, audit reports, and incident response teams are ways to find vulnerabilities in the system.

6.2 Don't Compromise On Quality For Cheaper Solutions

Not many organizations, especially SMEs, have the resources or funding to meet an eventuality where they must be right every time for protecting their data. In contrast, the cybercriminal must be right only once to perform a breach. Hence, it is prudent for businesses to be flexible with their budget because inexpensive and cheap are not always the same. Solution providers that come cheap may not be competent enough to handle advanced threats.

6.3 Check Security Certifications

Certifications help organizations verify the knowledge and qualifications of their cybersecurity professionals. Thus, checking and working on these certifications can help them discover new incident response techniques for advanced threat intelligence. The certifications help bridge the skill gaps of the IT teams, and they can boost productivity. The strength of the IT security team gets enhanced over time, and they can learn from the team members' expertise for faster responses.

Thus, checking the security certifications before purchasing a solution is a long-term investment, which is worthwhile for enhancing overall enterprise security.

6.4 Look at Independent Reviews

A cybersecurity review offers an in-depth and independent analysis of the organizational ability to shield its information assets. It aims to validate how effective cybersecurity measures are.

An experienced security solution provider performs a comprehensive audit of the measures that the organization implements. The review involves on-site and remote access. Conducting interviews with the senior managers is a part of the check to identify the relationship between the process, technology, and people. The report documents the current status of all security measures and determines the kind of cyber risk that the organization faces.

6.5 Purchase Cyber Insurance

In today's digital world, data counts itself in the list of critical business assets that standard property insurance firms do not cover. The value of information is often more than the equipment used to store it. A cyber insurance policy ensures that the data gets restored in the event of a cyber attack.

Organizations can face severe penalties if the users' credit card data gets compromised. Compromised retails are liable to bear the cost of re-issue of new cards, forensic investigations, and frauds. Even small companies may have to shell out vast sums of money running into thousands of dollars for such breaches.

Additionally, a standard policy doesn't cover the costs of electronic system downtime or a breach due to lost or stolen devices. Cyber insurance covers all these unwanted instances.

Final Words

It is common to hear about big businesses becoming a target of hackers, but the risk is the same for SMEs. Small companies do not have the financial aid and resources to bounce back after an attack. However, they can address the pointers mentioned earlier and choose a cybersecurity solution that best fits their needs.

References:

1. *Abi Tyas Tunggal, 2020, How to Perform an IT Cyber Security Risk Assessment, https://www.upguard.com/blog/cyber-security-risk-assessment*

2. *Robert Bond, 2017, Cybersecurity for Small Businesses, https://www.hitachi-systems-security.com/blog/how-to-find-inexpensive-cybersecurity-solutions-for-small-companies/*

3. *Karen Scarfone, Dan Benigni and Tim Grance, Cyber Security Standards, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153*

4. *Ben Canner, 2019, The Top 9 Cybersecurity Certifications, https://solutionsreview.com/security-information-event-management/the-top-9-cybersecurity-certifications-for-security-pros-in-2019/*

5. *Sadler Insurance, 9 Reasons Why You Must Purchase Cyber Insurance Now, https://www.sadlerco.com/9-reasons-purchase-cyber-insurance/*

Chapter-7

CISO as Service - The Perfect Cybersecurity Solution For Startups

For any organization to become successful, it needs a comprehensive and strategic Information security system that can efficiently safeguard the confidentiality, integrity, and availability (CIA) of its valuable information assets. To develop and maintain such a system, the organization needs to hire an in-house Chief Information Security Officer (CISO) or an external CISO-as-a-Service agency that manages the whole security system.

Hiring an in-house full-time CISO may not be an optimal choice for startups or small organizations. The primary focus of a new emerging organization is to put most of its resources in producing and launching new products and services to achieve initial business growth. At such a point, the expense of a full-time CISO is not affordable, and CISO as a Service seems to be a perfect cybersecurity solution for the startups.

7.1 What is CISO as a Service?

CISO as a Service is the resource through which the organization gets the information security leadership through appropriate technical support and a relevant pool of expertise. CISO as a Service guides the senior management in matters of information security and provides services like:

- Maintenance of information security system and management of risk in a cost-effective manner.
- Provides an extension to the information security capabilities of the organization.
- Prevents risks to the information network and offers a continuous security presence.
- Assessing the current information security posture and threat landscape.
- Identifies the digital information assets that need protection and analyses the level of security required.
- Developing an Information Security Strategy through which the necessary regulatory requirements can be implemented and maintained, risks minimized, and the level of protection improved.

7.2 Advantages of Using CISO as a Service

- **Expertise with Cost-Effectiveness**

Using CISO as a Service is one way through which an organization can enjoy the benefits of strategic security experience and technical skills without incurring much capital expenditure. Small organizations and startups don't need a full-time security expert, and CISO as a Service provides them the required experienced CISO expertise. If the organization chooses a CISO as a Service client who has a good client base, it will benefit from the client base's invaluable knowledge and expertise.

- **Independence**

The position of a CISO must be independent for properly managing IT operations, and he/she should be independent of office politics. To accomplish the objective, CISO as a Service is the best solution because of the unbiased perspective, along with a high amount of credibility that helps the organization in achieving its information security goals.

- **Continuity of Services**

The in-house CISO can get ill or could be hired by some other organization anytime. In such cases, business operations can be affected. CISO as a Service offers an organization the continuity of service. Even if one of the experts of CISO as a Service client moves, the relationship with the client continues, and another expert will manage the business operations.

- **Specialization**

Relying on a provider that offers a specialization in CISO as a Service will have a positive impact on the organization. The organization will benefit from the specialized areas of different CISOs of the client's organization. In short, the organization will get the advantage of the knowledge and experience of several CISOs in their specialized areas of expertise.

7.3 Qualities to Look For in a CISO

A reliable information security professional requires several skills as well as characteristics to be an effective CISO:

- **Leadership Presence**

A CISO must have the ability to represent the organization in matters relating to information security and must possess exceptional leadership qualities to influence the executives to work consistently to achieve the security goals as well as objectives.

- **Skills to Develop Strategies and Plan Programs**

A CISO should have the skills to prepare short-term and long-term operational plans to achieve security goals. One method is not enough to manage every situation. Hence, the CISO should have the skill to develop strategies by setting up priorities based on project-level risk.

- **Security Knowledge**

In-depth security knowledge is essential for a CISO as he/she will be the one who will represent the organization in various information security issues. Additionally, strong analytical, as well as problem-solving skills, are essential for a CISO.

- **Communicate and Delegate**

Creating a successful Information Security System is a team task. Hence, a CISO must continuously communicate with various individuals and teams relating to the security process. He/she should clearly define the decision-making powers of individuals to handle risk management decisions appropriately.

- **Creating Metrics Programs**

A CISO must develop metrics programs to analyze the performance and improvement in security functions. Conducting a periodic benchmarking process with other industry organizations can help compare various analytics and programs.

Final Words

It may not be affordable for startups and SMEs and will also be disadvantageous to have an in-house CISO in managing the organization's information security environment. In such a situation, CISO as a Service comes as a blessing. It provides flexibility in many ways, is cost-effective, and offers comparable results as hiring an in-house CISO. Understanding the differences involved in both modalities, and managing it appropriately, will be hugely profitable and can bring great success for a new enterprise.

Reference

1. IT Governance, Chief Information Security Officer-as-a-Service (CISOaaS), https://www.itgovernance.co.uk/chief-information-security-officer-as-a-service

2. Truvantis, Hiring a CISO as a Service, https://www.truvantis.com/ciso-as-a-service

3. Ethical Hat, CISO AS A SERVICE, https://www.ethicalhat.com/ciso-as-a-service/

4. Truvantis Blog, 7 Advantages of using a "virtual CISO" (vCISO), https://www.truvantis.com/blog/7-advantages-of-using-a-virtual-ciso

5. Bedel Security, Chris Bedel, Top 5 Benefits of a Virtual CISO, https://www.bedelsecurity.com/blog/top-5-benefits-of-a-virtual-ciso?hs_amp=true

6. Security Intelligence, Brian Evans, The Expanding Role of the CISO: Seven Attributes of a Successful Security Leader, https://securityintelligence.com/the-expanding-role-of-the-ciso-seven-attributes-of-a-successful-security-leader/

Chapter – 8

Ethical Hacking And Penetration Testing

Whenever people hear about hacking, they co-relate it to attacking someone's IT or network system for financial or personal gains. What people don't realize is that ethical hackers or white-hat hackers are professionals hired by governments and multi-national companies to locate vulnerabilities in information systems using the intent of an unethical hacker. Responsibilities of an ethical hacker [1] include developing scripts to test networks, using tools for security, performing risk assessment, training staff, and setting up security policies.

Penetration testing or pen testing is a part of ethical hacking since it exploits loopholes in a system to find whether malicious intrusions are possible. Ethical hacking is a broad area since it involves a massive network of systems. In contrast, penetration testing is limited to examining a few information systems.

8.1 The Benefits Of Penetration Testing

Pen testing is a simulated attack to reveal system vulnerabilities and gives a report regarding the weaknesses [2].

- Revealing Risks: Pen testers think like malicious hackers to identify vulnerabilities and categorize the associated risks into various categories such as high, medium, and low.
- Ensure Business Continuity: Testing reveals potential risks and avoids system downtime, which might comprise the business continuity.
- Expert Third-Party Opinion: Pen testing by outside professionals will help the management to get an unbiased opinion.
- Maintains Customer Trust: Performing pen tests frequently establishes trust with the clients since the business continuity is maintained, and also, there are fewer chances for monetary losses.
- Comply Rules & Regulations: Penetration testing verifies whether the system follows the rules and regulations published by the institution regarding data privacy and protection.

8.2 What Areas Should Undergo Penetration Testing?

During penetration testing, a tester tests everything from an individual computer down to its applications and even physical security. Testing is predominantly performed in four areas [3].

- Physical Security: Physical location of computers, routers, and other network devices is a critical factor since its site in unsafe places may allow intruders to steal the information by physically connecting devices to the network.

- Staff Awareness: Employees working in the firm should be alert and educated on how spam messages could compromise the system and identify malicious links and messages.

- Security Policy: A weak security framework of a company could make the intrusion easier for an attacker, and it is necessary to build a robust security framework consisting of all rules and regulations.

- Vulnerability Patches: It is the process of receiving patches from affected systems and securing such vulnerable areas for adequate security.

8.3 Some Free Penetration Testing Tools

Like a craftsman's toolbox, a penetration tester's toolkit includes tools to test a company's network based on their business objectives. Some of the top free pen-testing tools [4] are discussed below.

- Fiddler: Fiddler is a freeware web proxy tool primarily used to receive, interpret, and decrypt HTTPS traffic from systems.
- Metasploit: Metasploit framework is an open-source structure for robust penetration testing to uncover vulnerabilities in various platforms.
- Wireshark: Wireshark is a network protocol analysis tool that reads packets from a network and renders it in a human-readable form.
- Nikto: A web vulnerability scanner to identify outdated programs, server misconfiguration, insecure host, and version issues.
- Nmap: Nmap or network mapper is an open-source application for network scanning using IP packets. It can scan a range of IPs, ports, and subnets to identify loopholes.

8.4 Non-Traditional Penetration Testing Methods

Modern pen testing methods reveal critical security issues and also defines how such vulnerabilities can be fixed. Using such pen test methods requires expertise, and thus professionals are supposed to be dynamic and skilled.

8.4.1 Bug Bounty

A bug bounty [5] is a reward program for security freelancers and professionals for finding security flaws in the network of an institution. The bounty can be a financial incentive or a hall of fame recognition among co-workers or gear from the company or even a job offer.

8.4.2 Capture The Flag Challenges

Capture the flag (CTF) challenge [6] is generally a team-based cybersecurity competition to challenge the participants to solve a security-related issue and defend computer systems. Such competitions may range a few hours to even multiple days and include groups of students, scientists, and enthusiasts.

8.4.3 Advantages Over Traditional Penetration Tests

One advantage of a non-traditional pen test is its continuous testing [7], unlike periodic traditional pen tests, which sets the system to defend newer forms of attack. Secondly, the availability of thousands of enthusiasts makes the system resilient against almost all kinds of attacks. Finally, specialized experts are available at minimum cost for finding vulnerabilities that otherwise could result in massive IT spending.

8.5 Remedial Measures After Penetration Tests

For a successful pen test, it is necessary to plan and implement post-test measures [8] and then revisit the security framework. The post-test steps are as follows.

- Review The Test Results: Here, all the reports are converted into meaningful data for further discussions, and vulnerabilities are reported along with associated risks.

- Develop A Remediation Plan And Validate With Retest: Severity of risks are measured, and remedial measures need to be prioritized.

- Combine Findings Into Long-Term Security Strategy: Security weaknesses identified will be fixed to comply with the business security framework.

Final Words

The demand for ethical hacking and pen testers are hiking due to increasing cyberattacks. Modern tools and expertise have become a necessity today for addressing the changing landscape in the usage of sophisticated tools and techniques employed for security intrusions.

Reference

1. Lakshay Mor, Ethical Hacking and Penetration Testing Guide, https://www.simplilearn.com/ethical-hacking-and-penetration-testing-guide-article

2. Steven Wierckx, 7 Advantages of Penetration Testing,

https://www.toreon.com/7-advantages-of-penetration-testing/

3. EC-Council, 4 Areas that Every Penetration Tester should be able test,

https://blog.eccouncil.org/4-areas-that-every-penetration-tester-should-be-able-test/

4. Aseem Lodha, Top 10 Free Pen Tester Tools,

https://www.synopsys.com/blogs/software-security/top-10-free-hacking-tools-for-penetration-testers/

5. OSTIF, Bug Bounties – What They Are and Why They Work,

https://ostif.org/bug-bounties-what-they-are-and-why-they-work/

6. Aidan Knowles, Behind the Scenes at a Capture the Flag (CTF) Competition,

https://securityintelligence.com/behind-the-scenes-at-a-capture-the-flag-ctf-competition/

7. Triaxiom Security, The Advantages Of A Bug Bounty Program Over A Penetration Test,

https://www.triaxiomsecurity.com/2018/11/30/advantages-of-a-bug-bounty-program/#:~:text=Advantages%20of%20a%20Bug%20Bounty%20Program%3A%20Continuous%20Testing,at%20a%20point%20in%20time.&text=On%20the%20flip%20side%2C%20bug,typically%20open%20for%20continuous%20testing.

8. Core Security, Three Action Items to Consider After Completing a Pen Test,

https://www.coresecurity.com/blog/three-action-items-consider-after-completing-pen-test

Chapter – 9

Cybersecurity Guide According To Startup Maturity Stage

As mentioned in previous chapters, with limited resources and formidable competition, startups tend to invest less in cybersecurity frameworks than multi-national companies. However, with changing cyberspace, even smaller businesses have begun to share cloud infrastructures as mature companies do. It easier for a startup to execute and develop a cybersecurity model as the firm grows rather than employing a framework at the peak of the growth.

9.1 What Areas Should Startups Focus On?

Startups primarily focus on customer relations and sales, and this eventually causes security issues, and such businesses will be vulnerable to traditional malware attacks [2]. For securing data and customer privacy, such startups stress on three areas for improvised security.

9.1.1 Application Security

SMEs and startups ensure application security [3] by web application scanning, defacement monitoring, pen testing, firewall, and similar mitigation methods. The measures also include the following methods.

- Application distributed denial-of-service attack mitigation.
- Vulnerability patching using a web application firewall.
- Real-time monitoring, tuning, and remediation of attacks.
- Continuous scanning and pen test to find security flaws in applications.
- Application security for all the associated domains.

9.1.2 Infrastructure Security

Securing a company's infrastructure is as essential as securing data and protecting customer privacy. Corporates and startups achieve infrastructure security [4] in the following manner.

- Encrypting APIs and websites primarily using SSL.
- Protecting against DDOS attacks such as flooding the network.
- For distributed startups, it is safer to isolate network assets.
- Segregating network assets behind a firewall and utilizing access-level restrictions is another strategy.

9.1.3 People Security

Adequate security is based on how staff and customers behave, and this is enabled by understanding the threats and how it affects users. Startups achieve people's security [5] through various methods, as discussed below

- Developing a security culture by creating a security-savvy mindset among the workforce.
- Identifying security behavior for the workers.
- Embedding security behavior among employees using campaign materials.
- Professionalizing security using guard force and CCTV teams for maintaining security.

9.2 Cybersecurity By Maturity Stage

As intruders use sophisticated tools and techniques, startups must evolve in terms of cybersecurity to cope with any security issues. A mature cybersecurity model will reduce costs associated with breaches and incident response.

9.2.1 Zero To Minimum Viable Product

Startups are generally formed to address the pressing customer problems in their target market. Minimum Viable Product (MVP) [6] is a resourceful strategy for startups with limited resources and size. For small emerging companies, MVPs can be defined as the new product version, which helps the team collect maximum customer data using the least resources.

Moreover, startups at this stage will be in doubt of any available fund for business initiation. Startups use MVP to validate its growth and value hypothesis, and to measure the effect of MVP, baseline data is captured for further processing. Therefore, MVP helps startups to identify customer requirements in the least and efficient strategies.

9.2.2 Minimum Viable Product To Seed

In the second stage, customer data needs to be protected from receiving funding for startups. For achieving this, it is recommended to perform at least one pen test and implement a password policy for customers [7].

In addition to that, available data should be backed up in databases and encrypted when in-transit using virtual private networks. Besides, a password management policy should be developed to retrieve sensitive data onboard.

9.2.3 Seed To Seed A

Practically, this an active phase when startups establish robust security policies without affecting the business continuity. From this point, frequent pen tests should be performed, and it is suggested to employ a software development lifecycle [8] for security.

At this stage, unethical black-hat hackers may target startups. It is safe to continuously pen test the firm's network, limit access requests, implement an intrusion detection system at the host, and develop a disaster recovery plan. Moreover, periodic drills should be performed to educate the workforce and carry out a risk assessment exercise to simulate a real-world attack. Workstations are supposed to have updated anti-virus and mobile device management solutions.

9.2.4 Post-Series A

The final stage, post-series A, is where white hat hackers are employed in the firm, and business uses non-traditional penetration test methods like bug bounty. In terms of infrastructure security [7], the firm should have a security information and event management service tool.

A centralized account management tool can be used to manage system access requests and employ an IT team to manage employee's workstations using a security event management tool.

As the startup grows, the firm's cybersecurity framework must be frequently tested and updated to defend any cyberattacks. The success of the company lies with the way the organization handles the cybersecurity of personal data. Besides, it is easier for companies to develop a security framework at the beginning rather than implementing one during the development phase as it could create inter-operability issues and could affect business continuity in the worst case.

References

1. David Cowan, A comprehensive guide to security for startups,
https://www.bvp.com/atlas/security-for-startups#Too-small-to-worry-about-security
2. Foxypreneur, 4 Things Startups Should Know About Cybersecurity,
https://magazine.startus.cc/4-things-startups-know-cybersecurity/
3. Venkatesh Sundar, Application Security for Startups and SMEs,
https://www.indusface.com/blog/startup-application-security/
4. Eric, The startup's guide to securing your infrastructure,
https://blog.sqreen.com/startups-guide-to-securing-infrastructure/
5. CPNI, Optimising People in Security,
https://www.cpni.gov.uk/optimising-people-security
6. Shawn Carolan, Minimum Viable Product and the Importance of Experimentation in Technology Startups,
https://timreview.ca/article/535
7. Eugene Vyborov, Cyber Security For Startups: A Step-By-Step Guide,
https://www.forbes.com/sites/forbestechcouncil/2019/10/02/cyber-security-for-startups-a-step-by-step-guide/#312a1de52010
8. First Round Review, How Early-Stage Startups Can Enlist The Right Amount of Security As They Grow,
https://firstround.com/review/how-early-stage-startups-can-enlist-the-right-amount-of-security-as-they-grow/

Chapter-10

Recovering From A Cyberattack

Cybersecurity data breaches are becoming very common, and it is not always possible to avoid every attack because there is nothing like a fully-secured security system. Therefore, whenever an organization suffers a breach, it should be prepared to recover swiftly. Here are some steps that an organization should follow to respond and recover from a cyberattack to keep the confidentiality, integrity, and availability of its valuable information assets intact.

10.1 Responding To The Attack

Preventing or avoiding a cybersecurity incident from happening is always the best choice. However, incidents can occur due to unforeseen reasons. Hence, it is also necessary to have a cyber incident response plan ready to handle the situation of a security breach. Here are the steps that an organization must take to respond to a cyberattack effectively.

10.1.1 Stopping The Attack

Whenever a data breach occurs, an organization has to act quickly to minimize greater liability. The following steps can help in recapturing the organization's healthy environment of digital information handling and exchange.

- **Deploying The Incident Response Team**

The incident response team includes several internal stakeholders who have specific roles to play to control the situation:

- Technical workers investigate the security breach.
- Human resources, employee representatives, and intellectual property experts work together to mitigate the brand impact and recover the compromised data.
- Data protection experts and public relations representatives are also involved when personal data is compromised, such as customers' confidential and sensitive information.
- Legal advisors take care of the legal implications of the cyberattack and check whether the business insurance policies cover the losses.

- **Securing The Systems And Networks**

It is essential to follow the below steps without delay in case of detection of any data breach is detected:

- Ensuring that all the IT systems are working correctly.
- Isolating and suspending the compromised section or even the whole network of the organization if required, as the case may be.
- Searching and scanning the entire system and network to detect any other intrusions.

10.1.2 Restoring Data - The 3-2-1 Rule

The 3-2-1 rule of backup is a valuable and essential concept in data recovery. In most cases where there is a data breach, an organization can recover all lost or compromised data if it earnestly followed the 3-2-1 rule. Through this mantra, the organization ensures that its information is adequately protected, and sufficient backup copies are available if there is a need to restore the data. In many cases, data storage platforms fail, and adequate backing up of data using the 3-2-1 rule is the only safe option. The abbreviation 3-2-1 means the following:

- Three copies of data which consists of one original and two backup copies.

- Two different storage types to store the two backup copies so that one copy is available even if the other storage fails.

- One data copy must be stored at a remote location or offsite to minimize the chances of losing all the copies, even in a geographical or natural disaster.

10.1.3 Seeking Help Of IT Experts

While responding to a cyberattack, IT experts have an essential role in dealing with the cyberattack by employing various techniques and ensuring network integrity. The cyber and network security experts' main tasks involve:

- Monitoring the systems for detecting irregularities
- Installation and updating the firewalls as well as data encryption software
- Conducting penetration tests for preventing future attacks
- Establishing and maintaining more secured networks
- Developing security standards and best practices that should be followed by the organization for the prevention of cyberattacks

10.2 Recovering From The Attack

Once a response to the immediate problem in hand and containing the breach is made, the organization needs to recover from the damage caused by the attack and prevent such incidents from happening again. For this, considering the following things is essential:

10.2.1 Executing Disaster Recovery Plans

A Disaster Recovery Plan is a strategy executed in the event of any mishap or disaster of any kind that has affected the organization's working. The plan includes the step by step instructions that will help the organization to recover from the catastrophe. The instructions include:

- Process of restoring the data and information
- Which staff member needs to be working for the continuity of the business operations
- The IT partners and the roles they are going to play
- The communication protocols
- The roles and responsibilities of staff members and partners and other relevant instructions

10.2.2 Notifying Authorities Concerned

The mandatory regulatory notification requirement is necessary in the event of a security breach as many universally applicable laws and regulations, along with some industry-specific legislation, demand so. The organization also has to report the violation to all the organization stakeholders, including customers, business partners, investors, employees, and regulators.

10.2.3 Evaluating Cybersecurity Posture

The evaluation of the organization's cybersecurity posture is essential as it consists of the entire defense structure against the cyberattacks. The evaluation process includes the assessment of:

- Security policies put in place.
- Employee training programs to prevent cyberattacks
- Security solutions deployed, including anti-malware and antivirus programs and other relevant solutions that keep the cybercriminals at bay
- The security status of all the services, systems, networks, software, and hardware

10.2.4 Exploring Preventative Technologies

One of the core elements of the recovery process is the strengthening of cybersecurity management by exploring preventative technologies, such as:

- Multi-factor authentication
- Advanced data encryption programs to avoid threats from interception by malicious actors
- Maintaining and updating security software and hardware
- Full system backup programs that perform system backup regularly.
- Employing the right governance structure for developing, implementing, and monitoring the cybersecurity programs as well as policies
- Developing effective training programs

Final Words

However diligent and efficient an organization is in implementing cybersecurity measures, malicious interventions, and data breaches can still occur due to unforeseen reasons or some advanced hacking techniques capable of overriding all safeguards. Hence, it is always prudent to have adequate backups and other practical data recovery policies in place. Understanding the steps involved in handling the aftermath of a breach will significantly help any organization minimize the losses and avoid further damage to stakeholders and the computing environment.

References

1. Varonis, How to Respond to a Cyber Security Incident, https://www.varonis.com/blog/respond-cyber-security-incident/
2. Salt Lake Chamber, MBomis, Respond: 5 critical steps for responding to a cyber attack, https://slchamber.com/respond-5-critical-steps-for-responding-to-a-cyber-attack/
3. Malwarebytes Labs, What to do to recover from a cyberattack, https://blog.malwarebytes.com/101/2017/02/what-to-do-after-recovering-from-a-cyberattack/amp/
4. Shawn Tuma, Guide to Responding to Data Breaches and Reporting Cybersecurity Incidents to Law Enforcement and Governmental Agencies, https://shawnetuma.com/cyber-law-resources/guide-reporting-cybersecurity-incidents-law-enforcement-governmental-regulatory-agencies/#_Toc465982688
5. KeepitSafe, Trenton Baker, The 3-2-1 Rule for Cloud Backup, https://www.keepitsafe.com/blog/post/3-2-1-rule-for-cloud-backup/
6. SearchDataBackup, Margaret Rouse, 3-2-1 Backup Strategy, https://searchdatabackup.techtarget.com/definition/3-2-1-Backup-Strategy?amp=1
7. ECPI University, Cyber and Network Security Professionals Help Fight Cyber Attacks [INFOGRAPHIC], https://www.ecpi.edu/blog/cyber-and-network-security-professionals-help-fight-cyber-attacks-infographic?amp
8. ATG, How to recover from a cyber attack, https://www.atg-it.co.uk/cyber-security/recover-from-cyber-attack/
9. ATG, Jahmel, The Importance of a Disaster Recovery Strategy, https://www.atg-it.co.uk/uncategorized/importance-dr-strategy/
10. Security Scorecard, Phoebe Fasulo, What is a Cybersecurity Posture and How Can You Evaluate It? https://securityscorecard.com/blog/what-is-a-cybersecurity-posture
11. UpGuard, Abi Tyas Tunggal, What is a Security Posture and How Can You Evaluate It? https://www.upguard.com/blog/security-posture
12. Drooms Global, How to recover from a cyber attack, https://drooms.com/en/blog/how-to-recover-from-a-cyber-attack

Conclusion

A Verizon data breach report from 2018 states that 58% of all cyberattacks are targeted at small and medium enterprises (SMEs) or start-ups. And what's saddening is that most of these firms never manage to recover from such an attack.

An Accenture report states that 68% of businesses are perplexed because of ever-increasing security threats. And this risk becomes imminent when 2,244 attacks are happening every day with an attack launched every 39 seconds. More than ever in history, it is now that digital warfare is a real thing, and the sector that will be hit the hardest by such cyber attacks is that of SMEs and start-ups.

The misconception that small businesses won't be a target of ransomware attackers or hacker groups has often refrained companies from investing in cybersecurity measures. Such security negligence results have always come in the form of substantial financial loss, data loss, and the threat of further attacks like identity theft, ransom demand, money laundering, etc

The ebook Cybersecurity for SMEs and Startups addresses these security myths and provides an understanding of recent cyberattacks trends citing examples wherever necessary. This book is an endeavor to reduce the frequency of attacks or to better prepare small businesses for such attacks that might bring their operations to a complete standstill.

Having cybersecurity tools isn't the only way to keep attackers away. Spreading awareness among employees via training is as important as spending on security tools or antiviruses. Yet another pivotal primary measure entirely overlooked is the significance of having data back up. As attacks are rampant these days, it won't be a surprise if an attack takes place despite following the best security measures.

Once an SME or start-up is done with employee education and backing up their data, they need to understand the probable attacks that might target their organization. This ebook attempts to give a detailed analysis of the common cyber threats targeting SMEs and start-ups such as ransomware, phishing, APT attacks, DDoS, password targeting attacks, zero-day attacks, etc.

In the succeeding sections, the book acts like a guide that helps evade any of these attacks that might be a factor leading to the collapse of a flourishing SME or start-up. Ways of securing company networks are discussed at length, emphasizing the use of antivirus software, regular backup of data, data encryption, Two-Factor Authentication, Software updates, so on and so forth.

Furthermore, the book also highlights the best practices for maintaining cyber hygiene recommended by security experts. These include tips for ensuring email security, online safety, offsite cybersecurity, device security, and mobile security.

Since the battle against cyber attackers is a long and never-ending one, it is imperative to continue with security measures even if the human resources, energy, time or money involved seems like a drain to the pocket. An investment when things are normal can prevent something adverse from happening.

Hence, this book also discusses the more technical topics like using CISO as a service, benefits of penetration testing, options of free penetration testing tools, etc. Having a team of ethical hackers on board is a significant security step. With the right set of security experts, informed investments can be made to prevent and face any cyberattack that may target an SME or start-up.

This eBook provides a cybersecurity guide according to the start-up maturity stage. It furnishes a roadmap to security concerning a firm's position that comes handy when an organization finds itself in a dilemma.

Finally, after talking extensively on the types of cyberattacks and the means of avoiding them, the book talks about another crucial aspect of cybersecurity, which is seldom discussed.

The eBook outlines the ideal ways of dealing with a cyberattack. Recovery from an attack isn't always guaranteed. Still, with the correct approach, the impact of an attack can be reduced significantly. The book explains how to respond to an attack, stop an attack, and restore data using the 3-2-1 rule. The role of seeking the help of IT experts in ensuring recovery from an attack is also discussed.

In conclusion, the eBook Cybersecurity for SMEs and Start-ups suggests time-tested Disaster Recovery Plans. It stresses other security measures to ensure that small and medium enterprises or start-ups do not succumb before the malicious plans of cyber adversaries.

About CyberPeace Foundation

CyberPeace Foundation (CPF) is a global civil society organization, think tank of cybersecurity and policy experts with the vision of pioneering CyberPeace Initiatives to build collective resiliency against cybercrimes and global threats of cyber warfare. CPF is involved in Policy Advocacy, Research and Training related to all aspects of CyberPeace and Cyber Security. Key areas of CyberPeace Foundation's work are in Technology Governance, Policy Review and Advocacy, Capacity and Capability creation and building through partnerships with various government organizations, academic institutions and civil society entities.

About Autobot Infosec Pvt. Ltd.

A global cyber security services firm providing a full range of data security services. We work with corporations and Governments in areas of Homeland/National Security, Enterprise Security; its work includes policy and strategy development, product / solution based professional services.

About UN Global Compact Network India

Global Compact Network India (GCNI), the Indian Local Network of the United Nations Global Compact (UNGC), New York is the first Local Network globally to be established with full legal recognition. As the UNGC local arm, GCNI has been acting as a country level platform in providing a robust platform for Indian businesses, academic institutions and civil society organizations to join hands for strengthening responsible business practices. Our '10 Principles in areas of Human Rights, Labour, Environment and Anti-corruption' provide a common ethical and practical Framework for Corporate Responsibility - and the 17 'Sustainable Development Goals (SDGs)' adopted in September 2015, by all 195 Member States of the United Nations including India in order to end extreme poverty, fight inequality and injustice, and protect our planet- understood and interpreted by businesses around the world , regardless of size , complexity or location.

About Institution of Electronics and Telecommunication Engineers (IETE)

The Institution of Electronics and Telecommunication Engineers (IETE) is India's leading recognised professional society devoted to the advancement of Science and Technology of Electronics, Telecommunication & IT. Founded in 1953. The IETE is the National Apex Professional body of Electronics and Telecommunication, Computer Science and IT Professionals. It serves more than 1,25,000 members (including Corporate, Student and ISF members) through various 64 Centres, spread all over India and abroad. The Institution provides leadership in Scientific and Technical areas of direct importance to the national development and economy. Government of India has recognised IETE as a Scientific and Industrial Research Organization (SIRO) and also notified as an educational Institution of national eminence. The objectives of IETE focus on advancing electro-technology. The IETE conducts and sponsors technical meetings, conferences, symposia, and exhibitions all over India, publishes technical journals and provides continuing education as well as career advancement opportunities to its members.

CyberPeace Foundation | Autobot Infosec | UN Global Compact Network India | INDIA

L29 - L34, First Floor, Connaught Place, New Delhi, Delhi 110001

www.cyberpeace.org | secretariat@cyberpeace.net | +91 957 0000 265

www.autobotinfosec.com | info@autobotinfosec.com | +91 957 0905 555