Cybersecurity Management in Small and Medium Sized Enterprises

Surendar venkatachalam
ITMS 578, cybersecurity management
A20525010
svenkatachalam@hawk.iit.edu

Abstract :

The industrial environment is changing dramatically as a result of Industry 4.0 and the essential digital transformation. Small and medium-sized firms (SMEs) continue to employ cutting-edge Industry 4.0 technology in order to boost their competitiveness. Meanwhile, small and medium-sized businesses are a common target for cybercriminals because they often have little resources and lack the skills to manage cybersecurity concerns. Regardless of the various cybersecurity principles or frameworks already in place, small and medium-sized businesses are the most vulnerable to cyber assaults. This research will provide an overview of the issues that small and medium-sized enterprises face when developing cybersecurity policies, as well as the possible cyber-attacks that they may face as a result of failing to create a more secure infrastructure.

Keywords : cybersecurity management, Incident Response, Risk Assessment, cyberattacks.

1. Introduction

Cybercrime is an increasing threat in the Small and Medium Business (SMEs) environment. The reliance of SMEs on information technology and the Internet has created vulnerabilities to cybercrime. Because of these flaws, information security has become a crucial concern for all SMEs. Because of their customer relationships with larger corporations, SMEs can be tempting targets for hackers. The growing number of cyberattacks on Small and Medium-Sized Businesses (SMEs) and the fact that these businesses frequently do not deploy effective defenses against attackers due to limited economic resources and a shortage of skilled security workers necessarily requires the implementation of relevant cybersecurity actions in SMEs. Urge to enhance cybersecurity is frequently low in SMEs since the necessary information and

awareness to generate motivation is typically lacking.

1.1 Definition for small and medium-sized enterprises

Small and medium-sized companies (SMEs) are firms with sales, assets, or a particular number of workers that fall below a specified threshold. Each country defines a small or medium-sized firm differently. Some size criteria must be satisfied, and the industry in which the firm works is occasionally considered.In this setting, one of the most significant functions of SMEs is poverty reduction through employment creation.

Developed as well as developing countries are taking extreme benefits from SMEs that are capable of accelerating the economy of any country. The majority of today's larger corporations grew out of small and medium-sized businesses. SMEs vary from large firms in three ways: unpredictability, innovation, and evolution. The SME sector is divided into three categories: micro-businesses, small enterprises, and medium firms. SMEs are the beginning point for economic development in the direction of industrialisation. SMEs, on the other hand, have a considerable impact on income distribution, tax revenue, employment, resource efficiency, and family financial stability. The only sustainable approach to decrease poverty is to support economic growth through wealth generation and job creation. SMEs are the primary source of revenue in developing nations, as well as a breeding ground for entrepreneurs and a source of employment.

1.2 Cybersecurity management

The activity of developing and implementing a unified data security plan to safeguard vital systems and sensitive information from digital threats is known as cybersecurity management. Because of the significance of this occurrence in various domains, including national security and the global trade system, cybersecurity has recently become a front-page IT technology concern. Mainstream businesses usually have complex IT systems. Staff members may log in from the workplace or from home because the average tech stack contains both on-premises and cloud services. Its complexity can lead to new attack channels for hackers as well as new data security issues for businesses.

Without a cybersecurity plan, your firm cannot protect itself from data breaches. Your firm becomes a great target for cyber thieves in the absence of adequate cybersecurity management procedures.Cybersecurity management is developing and executing a unified data security plan to ensure that data stays secure regardless of how the company's infrastructure changes.

Risk assessment, security rules, personnel training, an incident response strategy, and frequent audits and testing should all be part

of a cybersecurity management framework. Organizations may avoid financial losses, secure personal data, and retain their brand by creating a strong cybersecurity management structure.

1.3 Importance of cybersecurity management for small enterprises

SMEs' reliance on information technology has also rendered them exposed to modern information security concerns. Because of their customer relationships with larger corporations, SMEs can be tempting targets for hackers. Protecting SMEs from cybercrime and security issues should thus be a major priority for SMEs. As a result, it is critical for small businesses to prioritize cybersecurity management in order to secure their digital assets and maintain the long-term viability of their organization.

Cyber security has become a must for businesses of all sizes as bad actors have attacked their systems and networks carrying sensitive and valuable data. All forms of data have to be protected against theft and damage. Your business cannot protect itself from online dangers without a cyber security strategy, leaving it vulnerable to criminals who regard your business as an easy target. The inherent and residual risks have steadily increased with the development of technology. Big corporations have embraced more convenient means of carrying out their operations; for example, data may now be kept on the cloud; many businesses employ cloud services such as Amazon Web Services to store their valuable data. Despite being useful, businesses rarely adequately protect their information when using these cloud services.This has increased the risk that your company may fall victim to a successful cyber-attack or data breach, combined with an increase in attacker sophistication.

Businesses cannot rely on straightforward defenses like antivirus software or firewalls to protect themselves from the looming threat of cybercriminals, who are getting better and better at getting around these fundamental safeguards. Businesses should collaborate with a cyber security provider to develop a cyber security plan capable of offering multilayered protection.The fact that cybercriminals do not distinguish between different types of organizations means that all firms, regardless of size or industry, should take cybercrime seriously. This is particularly true for businesses in highly regulated sectors like healthcare or finance.

2.1 Problem and Significance

2.1.1 Current status

SMEs, like major enterprises, are always exposed to many hazards; more crucially, their survival is more fragile at any one time due to the limited quantity of their financial and nonfinancial resources. Typically, the company plans pay little attention to risk

management implications, even though numerous strategic movements, such as avoidance, control, and collaboration, can minimize uncertainty. Currently, risk management has become a severe issue that often impacts the performance of SMEs for a variety of reasons, including a lack of resources and a lack of procedures to support their risk management activities in general.

SMEs did not appear to be concerned with the normative pressure exerted by the cybersecurity community, such as through professional practices. Thus, authorized personnel frequently participate unintentionally in unsafe behaviors which could damage the institutions' security, privacy, data and current technical preventative measures. Because of the lack of SMEs' participation in the research community and the information garnered from the large enterprises' environment, most cybersecurity experts believe that the existing security techniques utilized by SMEs may be a hindrance to efficiency. More training activities, it has been suggested, would enhance knowledge, but this would not always translate into appropriate cybersecurity practices. As a result, SMEs will continue to be a favored target of individuals wanting to profit from cybercrime until there are meaningful changes in procedures and regulations to address the issue.

Users of SMEs are most often unaware of the various forms of cyberattacks, which has a significant impact on their awareness of cybercrime. As a result, workers' activities may eventually influence the success or failure of the company's cybersecurity operations. SMEs must be aware of the ramifications of cybersecurity and work to solve them, since this understanding may lead to the adoption of appropriate actions. More than tool installation for analyzing self-assessed risks, SMEs require additional knowledge about potential vulnerabilities; hence, they should design the content of their specialized awareness programs immediately.

2.1.2 Types of cyberattacks an enterprise may face

Describing cybersecurity threats in SMEs could be a critical solution for assisting SMEs in understanding the fundamental concept of cybersecurity. Cyberattacks against SMEs' assets, such as data breaches, data loss, and restricted access to the data, often have a negative impact on various of the business's activities. Nonetheless, numerous indicators suggest that SMEs underestimate cyber threats by failing to implement effective security measures. Ransomware, data breaches, phishing attacks, smart grid assaults, IoT attacks, and even state-sponsored attacks are becoming increasingly widespread in small and medium-sized businesses.

Malicious HTML emails, web server compromise, data loss on portable devices, inadequate configuration management, insider threats, a lack of contingency planning, as well as cyber-attacks that take

advantage of open vulnerabilities and staff members' careless use of the internet, wi-fi, or publicly accessible networks are some of the most frequent cyber threats that SMEs face. These assaults make advantage of compromised assets such end-point operating systems, email-opening devices, websites or servers, mobile devices, company databases, employee-owned devices within the company, the complete corporate network, IT infrastructure, and regulations. The stated difficulties may impede SMEs' ability to develop an effective security policy to secure their data and online services.

2.1.2.1 Phishing attacks

Small companies may be devastated by phishing attempts. These can result in the loss of sensitive data as well as financial damages. These attacks might potentially harm your company's reputation. Phishing assaults might even result in legal action being taken against your company in rare situations.

Attackers instill a sense of urgency or panic in their targets in order to get them to comply with their demands. They are constantly improving their strategies in order to make them more difficult to identify and defend against. And they now have a plethora of new platforms from which to start their phony activity. The development of services like WhatsApp, Slack, Twitter, and LinkedIn has increased the attack surface. And new platforms are always emerging. For example, there was a boom of fraudulent Zoom invites during the epidemic.

Web session hijacking, email customization, link masking, and email thread hijacking are examples of developing dangers. And hackers are using them not only on the desktop/email, but also on developing channels like Voice over Internet (VoIP), Short Message Service (SMS), and Instant Messaging (IM). Evidently, orienting an organization's defenses around office technology might make assaults more difficult to detect and resist. In recent years, phishing assaults have become considerably more sophisticated, with attackers becoming more convincing in impersonating real business connections.

To avoid future phishing attempts, educate your staff about the risks of clicking on links and opening attachments from unfamiliar sources. Workers should also understand how to identify a phishing email. Check that your company has effective anti-spam and anti-virus security in place. Also, keep your security software up to date and teach your personnel on how to utilize it. Prepare a strategy for what to do in the case of a phishing assault. This should include who to call and what measures your company should take to mitigate the harm.

When it comes to limiting the dangers of phishing, multi-factor authentication (MFA) is also critical. When users enter into an account, MFA adds an extra layer of protection to the authentication process. Even if an attacker is able to compromise an

account login and password through phishing, they will be unable to access your account without that extra piece of information known only to the user if MFA is enabled.

2.1.2.2 Malware attacks

Malware is the second most serious hazard to small companies. It contains a wide variety of cyber threats such as trojans and viruses. Malware is frequently distributed by malicious website downloads, spam emails, or by connecting to infected workstations or devices. These assaults provide attackers with a back door into data, putting consumers and employees in danger. Small businesses like to recruit staff who use their own devices for work since it saves time and money. It is a common practice in lot of firms, its termed as BYOD(Bring your own device). This, however, makes them more vulnerable to malware assaults, as personal devices are far more susceptible to fraudulent downloads.

One of the most prevalent botnet assaults is on a website. The majority of Businesses have a website via which they engage with their consumers. The website may be susceptible if it has badly designed custom code, which allows attackers to exploit several security weaknesses. Attackers can infiltrate the corporate website and use it as a slave server to disseminate malware unintentionally. Another concerning new development is malware's ability to take over auto-fill capacity forms on a website. Auto-fill is intended to make filling out forms easier, however, it may be exploited by malware. Several experts recommend that users disable auto-fill applications in browsers such as Chrome, Safari, and Opera.

Companies may avoid malware attacks by putting in place strong technological safeguards. Endpoint Security systems safeguard devices from malware downloads and provide administrators with a centralized control panel from which to manage devices and guarantee all users' security is up to date. Online security is also critical since it prevents people from visiting harmful websites and installing hazardous malware.

2.1.2.3 Ransomware attacks

Every year, ransomware, a sort of cyberattack, damages hundreds of enterprises. Being one of the most profitable sorts of attacks, they have only risen in popularity. This is a scenario in which a firm receives an email, clicks on a link, and discovers that its computers are frozen. A malicious email may contain a link to a website offering a malicious download or an attachment with downloader capability built in. If the email recipient falls for the hoax, the ransomware is downloaded and run on their machine. After ransomware has obtained access to a system, it can begin encrypting its data. Because an operating system has encryption capabilities, this simply comprises accessing files, encrypting

them with an attacker-controlled key, and replacing the originals with encrypted copies. Most ransomware strains carefully select which files to encrypt in order to ensure system stability.

The cybercriminal offers to remove the ransomware in exchange for money. In general, ransomware attacks of all sizes follow the same fundamental principles: attackers capture and lock a company's data or assets and offer to restore them upon payment of a ransom. As their data is usually not backed up and they need to be operational as soon as possible, smaller businesses are much more inclined to pay a ransom.

To stop these attacks, businesses need to have strong endpoint protection in place across all corporate devices. This will aid in preventing ransomware assaults from effectively encrypting data. Companies should also consider using an effective cloud backup solution. The danger of data loss is decreased by these solutions' safe cloud backup of company data. Organizations can use a variety of data backup strategies, therefore it is critical to investigate the approach that will work best for your firm.

2.1.2.4 Insider attacks

The insider threat is the last significant danger facing small firms. An insider threat is a risk to a firm posed by employees, former employees, business contractors, or sympathizers. Because insider threats can go unnoticed for extended periods of time, sometimes even years, they are considered to be extremely deadly. Businesses might wrestle with the difficulty of figuring out whether they are engaging with that data in a harmful, or beneficial, fashion as part of their job activities since they involve someone who already has access to the leaked data.

Financial gain is the main motivation for insider threats, as it is for the majority of cyberattacks and threats. These individuals have access to sensitive information about your company and have the capacity to inflict harm out of greed, malice, or even simple ignorance. Accidental data breaches may result from staff members' or partners' unintentional acts and behaviors when they have access to your sensitive data. Malware specifically targets online social networks, and employees using workplace computers to browse social media sites run the risk of infecting the whole company network.

Small businesses must ensure that their organization has a strong security awareness culture if they wish to avoid insider threats. Limiting access to sensitive information is essential for preventing any kind of insider threat, whether purposeful or inadvertent. Establish rigorous guidelines for who and how may access important areas, and make sure that each of your workers only has access to the system and data they require to carry out their daily activities. Access to your company's network and their employee accounts need to be terminated as soon as the termination process is through, and they need to be watched for a specific amount of time after leaving. As a consequence,

employees will be able to detect an attacker who has breached or is attempting to access business data early on, assisting in the prevention of insider dangers caused by ignorance.

2.1.3 Effects of cyberattacks on Small and medium enterprises

Every firm can suffer catastrophic effects from cyberattacks, but small businesses are particularly vulnerable. Unprepared small firms may have to cope with severe financial consequences as well as harm to their brand, pricing strategy, productivity, staff morale, and other factors when a cyberattack occurs.

The company would suffer immediate financial losses as a result of a cyber assault, such as the expense of retrieving data, fixing damaged systems, and hiring legal and public relations professionals. Cyber assaults can result in legal, civil, and regulatory penalties, leaving a company's operations and future unknown. Any of these charges, and others, can reduce a company's worth. Moreover, firms may be required to retain attorneys and other professionals in order to comply with cybersecurity rules. If they are the victim of an assault, they may have to pay even more in legal costs and damages as a consequence of civil proceedings filed against the corporation. In addition to direct expenditures, cyberattacks include secondary costs such as unanticipated downtime, lost production, and lowered morale. Operations might come to a standstill, especially if you rely on vulnerable web-based apps.

Businesses must reconsider how they acquire and retain information to guarantee that sensitive information is not compromised. Cyberattacks may significantly harm a company's reputation. Customers may be reasonably afraid about visiting establishments that have been targeted by terrorists. Similarly, investors may see being a victim of a hack as a sort of irresponsibility and may avoid getting involved.

2.2 Challenges for small and medium enterprises in cybersecurity

The basis in all of these problems seems to be management understanding and commitment, which in turn govern budget, resource allocation, and efficient use of cybersecurity procedures.Implementing cybersecurity in SMEs faces challenges such as a lack of management support due to other corporate objectives, a limited budget, and a lack of resources with technical expertise and cybersecurity solutions.

2.2.1 Lack of awareness

Individuals can be careless with security, disregarding it and doing little to address the dangers. They might also be worried, taking some precautions but being content with the bare minimum rather than transitioning to a

concerned attitude in which they do all necessary to safeguard themselves. Small firm owners frequently lack a thorough awareness of information risks and information security requirements under industrial and regulatory standards. Lack of awareness of cybersecurity amongst employees is a tragedy waiting to strike businesses.

Employees are ignorant of the risks they encounter on a daily basis in a time of rising danger from hackers. Lack of employee awareness leads to most threats for SMEs like phishing, malware attacks, and social engineering. These scenarios get elevated with employee negligence, which is using weak passwords which are easy to guess and using the same passwords for multiple accounts in the worst case scenario writing and sticking it on a piece of paper in the workplace. In the same case scenario connecting a work computer to a public network also proves to be fatal as well.

2.2.2 Limited budget being allotted for cybersecurity

Most SMEs repeatedly cited budget as a barrier to implementing effective cybersecurity systems. Small business cybersecurity is frequently a "do the best with what's available" scenario, as opposed to bigger organizations with significant IT expenditures. Many SMBs lack the financial resources to implement typical corporate security policies. Often, a company's IT budget, which takes into account factors like company size and IT infrastructure, is linked to the real cost of cybersecurity. Small firms can have limited resources, and occasionally the person responsible for planning and approving the budget may be unaware of the need for cybersecurity.

Cybersecurity is no longer a "nice to have" for businesses; it is a "must have," and it must be budgeted for. It is crucial to emphasize, however, that cybersecurity protection is not just a function of money invested. A complete cybersecurity program does not have to be expensive, but it does need focus and commitment from management, IT, and staff. On the other hand, no matter how much money a corporation invests in upgrading its cybersecurity posture, there is no such thing as 100% protection. A company's best hope is to implement a holistic, continuous cybersecurity program that combines resources, testing, training, and time to help keep them cyber strong and perhaps reduce expenses in the event of an attack.

Enterprises often devote the majority of their budgets to existing initiatives and prioritize spending on business activities that create money for the organization. This results in a lack of financing for network and IT infrastructure that protects IT assets from external threats. Cybersecurity measures are frequently overlooked because SMEs do not consider security as a critical component of day-to-day business operations.

2.2.3 Limited Resources

In general, SMEs don't normally have as many resources as huge corporations do; in certain cases, the situation is even reversed. Lean teams with a lot of work to complete are common in new, small, and expanding Enterprises. Because of this, SMEs must carefully choose their priorities to make the most of their resources—money, talent, and time. By no means, though, is security an SME's top priority. SMEs must divide their scarce resources among a variety of important projects. Security occasionally slips down the list of priorities since the solutions that are available are frequently designed for companies (they are expensive, complicated, and need extensive in-house knowledge to administer).

Small businesses, in general, devote more resources to core company tasks such as project execution, marketing, and finance. SMEs' IT departments have extremely few employees; moreover, the resources are poorly educated and are unaware of the most recent cybersecurity dangers.

The operating costs of SMEs rise as they expand. With increased expenditures and new processes to enable continual expansion, cybersecurity is frequently the last thing on their minds. Here is where many Businesses make disastrous mistakes.

2.2.4 Inadequate training for employees on cybersecurity

If your budget is restricted, you will be unable to recruit the most experienced and/or competent individuals. Many SMEs are defended by teams that lack the institutional knowledge, cutting-edge abilities, and broad experience that great enterprise teams possess. These teams may not be able to undertake a comprehensive and sophisticated cyber vulnerability assessment. Hackers, who appear to be becoming savvier and more numerous by the year, recognize this weakness and exploit it by launching complex assaults that less experienced teams struggle to fight against.

When it comes to cybersecurity, employees are frequently the weakest link. By clicking on a malicious link that appears authentic, they might unintentionally let hackers sneak through the cracks and wreak havoc on a company's infrastructure. To avoid this, the most important action SMEs could do is to educate their personnel on security, protocols, and processes. Employees will benefit from regular cybersecurity awareness training in order to manage passwords, recognize and avoid phishing attempts, and learn about a variety of other dangers and critical security measures. This training is best delivered through presentations and drills. DDoS assaults, installing unauthorized devices, phishing emails, internal and external network scans, tabletop exercises, and other activities are examples of drills.

2.2.5 lack of proper cyber infrastructure models in SMEs

The cyber security business has evolved in reaction to the risks posed by cyber-attacks, with government and major corporations leading the way since they both represent the most valuable target and are the sectors best able to finance the development of cyber defenses. The discovery of vulnerabilities leads to cyber security measures, with solutions ranging from software updates to security-specific tools, professional people, and business procedures. If the financing or prospective purchasing power required for the creation of cyber security measures comes from the government and major industry, vulnerability researchers will look for issues inside the government and large industry-type infrastructures.

One of the observed challenges is SMEs' inability to link cybersecurity deployment to business goals, demonstrating the necessity of the solution for securing domain-specific mission-critical assets. Even if a business has not accepted any current cybersecurity standard or framework, there is a good likelihood that they have established some type of security measures.

3. Approaches to mitigate cyber threats in Small and medium enterprises

Cybercrime is a real concern today, yet SMEs continue to deny it. As long as SMEs approach cybersecurity in this manner, the issue may get more difficult in the future. SMEs are more vulnerable to cyberattacks as a result of their adoption of low-cost cybersecurity practices. In most situations, Businesses suffer from cybersecurity risk management owing to components of their goals and plans. As a result, raising cybersecurity knowledge at the managerial level of SMEs may enhance other significant elements such as behavior and decision-making. For example, raising decision-makers' knowledge might lead to more SMEs investing in cybersecurity.

In contrast, cybersecurity procedures are an important component that might give an ideal solution for SMEs. Some cybersecurity risk assessment approaches have been customized to be suited for smaller enterprises in order to meet the demands of SMEs. Maturity models are also frequently used owing to their capacity to give a comprehensive evaluation while adapting based on SME characteristics. The problem with all of these techniques is that they all presuppose a certain degree of cybersecurity competence at the SME and that they are working with a motivated user. Although these assumptions may be valid for digital enablers and digitally based Businesses, they cannot be anticipated by digitally reliant SMEs and start-ups, who usually have little to no cybersecurity understanding and are hence unmotivated to improve their cybersecurity condition.

3.1. Develop a cybersecurity policy

A Cybersecurity Policy is developed to provide behavioral guidelines for businesses and their workers in order to establish and maintain a secure culture. They provide the methodology for how workers and other firm stakeholders should adopt security behaviors in their daily jobs. Furthermore, these protocols outline how to respond to threats and adopt tactics to prevent vulnerabilities and recover from an attack if one happens. Every business, regardless of size, must have a Cybersecurity policy.

Developing a strong, dynamic information security policy necessitates collaboration across all main business pillars. The best place to begin is with a cyber risk assessment of the company. Decision makers must identify any locations in the system where data confidentiality, availability, or integrity might be compromised. Moreover, it is critical to identify any possible risk in operations - this might be supplier chains, the business model itself, or any other weaknesses - and comprehend the implications of a data breach in these areas.

3.2. Implement more security practices

Protect accounts with elevated rights, remote access, and/or utilized on high-value assets first. To augment knowledge-based elements such as passwords and PINs, physical token-based authentication solutions should be utilized. Companies should move away from single-factor authentication, such as password-based systems, which are vulnerable to credential theft, falsification, and reuse across various platforms due to poor user choices. Firewalls serve as a barrier between the outside world and your network, giving your company more control over incoming and outgoing traffic. Likewise, antivirus software scans your device and/or network for possible dangerous threats.

You should also protect your networks from cyber threats by deploying firewalls, as this is where nearly all attacks begin. A reliable system will successfully protect you against brute force assaults or prevent security incidents from causing long-term damage. Moreover, firewalls monitor your network traffic for any unusual behavior that might jeopardize the integrity of your data. They also safeguard your PCs from sophisticated threats and promote data privacy.

Use considerable caution while deciding which firewall is best for your company. Choose a solution that provides you with complete security control and visibility over your application and networks. It should also be capable of protection and prevention, as well as a simplified security architecture. Firewalls serve as a barrier between the outside world and your network, giving your company more control over incoming and outgoing traffic. Likewise, antivirus software scans your device and/or network for possible dangerous threats.

3.3. Backing up the data

Making a duplicate of your data to use in case the original is lost, destroyed, or becomes inoperable is known as a data backup. Your vital data is protected from illegal access by the additional encryption layer provided by your backups. One of the most crucial measures a business may have to avert long-term damage after a data breach is trustworthy backups. Depending on how frequently you back up data, if your organization, for instance, has a ransomware attack and all of your data is encrypted, you may only be at danger of losing one week's worth of data or less if you have high-quality backups. You could be forced to pay the ransom or shut down your firm entirely, as compared to a corporation that only does it every six months or never.

Data is today regarded as one of a company's most significant assets, as was previously noted, thus it should make sense to take every precaution to preserve it. By doing regular backups, you can make sure that your company can continue to run even in the event of a flood, fire, physical injury, or theft. Also, you won't be extorted by ransomware attacks if you have backups of your data that you can access right away.

3.4. Providing cybersecurity training to employees

Since they have direct access to your networks, employees and their communications connected to their jobs are one of the main causes of data breaches for small firms. Cyberattacks may be greatly reduced by providing staff with training on fundamental internet usage and practices. Human mistake is the main cause of malicious firewall and ransomware assaults. Some of them were even brought on by your staff. Phishing emails sent to your workers are one of the typical methods criminal hackers acquire access to your information.

Phishing emails are hard to recognize because they seem genuine. For instance, a hacker may send an email asking for personal information while impersonating the leader of the company. The worker might end up disclosing this information if they weren't given the proper training. You must do cybersecurity awareness training because of this. Inform your staff of the main types of cybersecurity attacks and the best defenses against them.

The significance of double-checking email addresses before responding to them and links before clicking on them should also be emphasized. The company policy about sharing sensitive information, including on social media, should also be highlighted. Regular training is the greatest approach to lower the possibility that your team may pose a security concern. All members of your team should participate in this training, not just your cybersecurity and IT employees, since any one of them might end up becoming a weak point in your business operations. When properly taught, you can reduce security risks from social engineering assaults like phishing and scam emails.

3.5. Staying updated about latest technologies

Operating systems, antivirus programs, and other commonly used software are updated often by the companies that provide them. These upgrades are necessary for the continuing usage of these programs, whether they enhance existing capabilities or reduce security risks. You can stay safe from recently identified malware, viruses, and third-party vulnerabilities by installing these updates. You ought to automate this, ideally. When a fix is made public, cybercriminals may almost immediately start working on vulnerabilities. Several companies provide update services that can aid with automation; just be sure to utilize updates sent over secured links and to test them before releasing them in production. Your cyber security and digital safety are significantly impacted by software and system upgrades. This is because they don't just add new features; they also fix bugs and aid in patching exploitable security flaws and vulnerabilities.

3.6. Conducting security assessment more frequently

Determine if your critical infrastructure is protected against security breaches by conducting a security assessment. Also, you should examine your data protection strategy and see whether it includes data disposal procedures. Companies should strive to regularly conduct cyber risk assessments as technology continues to develop and change. Doing so may help you find any possible weaknesses in your company's security measures. A risk analysis can provide information on the assets that need to be safeguarded and the security measures that are already in place. The IT security team at your company may discover possible vulnerability points and prioritize which weaknesses need to be fixed first by conducting a cybersecurity risk assessment.

A cybersecurity risk assessment is the first step in improving company security, which is made more important by the growth in cybercrimes. Using this type of security test has advantages beyond protecting important data, such as raising awareness, reducing risks, and improving communication.

3.7. Develop an incident response plan

It may be easier to have resources set up and ready to go if everyone, including the IT security team and non-technical workers, is aware of their roles in the event of a data breach or attack. The main priority in your strategy should be business continuity, followed by data protection, data restoration, offshore backups, system reconstitution, configurations, and logs. Frequent evaluations of your whole cybersecurity risk management plan may assist you in identifying issues. A firm should have a plan in place for catastrophe recovery. A disaster recovery plan ensures that your IT and staff teams know what to do in the event of a

breach. It seeks to reduce the amount of time you spend offline so that your operations can resume as soon as possible. An incident response plan allows your company to be proactive by taking all necessary precautions so that your team can respond quickly and effectively to any problems.

4. Conclusion

What has been shown in this study is that the Less digitally mature Small- and Medium-Sized Enterprises (SMEs) are the most vulnerable to cybersecurity threats of all organizations because they lack the necessary cybersecurity knowledge, awareness, and resources to deal with cyber-attacks. Even more concerningly, they frequently lack the incentive to strengthen their cybersecurity posture due to their insufficient understanding of the subject. The importance of information security in any business cannot be understated as security risks can become threatening to the existence of the business itself if not dealt with accordingly.

Each argument in favor of implementing cybersecurity defenses is driven, either directly or indirectly, by a specific danger. Businesses must create effective cybersecurity management strategies since a lack of competent cyberinfrastructure and management might leave them open to assaults. But it’s not like they are vulnerable to all kinds of attacks. Every company would have some sort of cybersecurity protection in place depending on the budget being allocated. But the implication is that they are not enough to protect a company from all kinds of attacks. As we discussed earlier there is no 100 percent protection in cyberspace, it's about how we react to it and how we recover from the incident. It’s not easy to find and implement proper cybersecurity measures for any SME, But with the right approach to cybersecurity management, SMEs can safeguard their operations, reputation, and customers, and continue to thrive in today's digital landscape.

5. Future work

The use of artificial intelligence (AI) and machine learning (ML) has become crucial in many industrialized nations in laying the groundwork for the future of data management and security in the SME sector. In these industrialized nations, SMEs have established their cyber systems based on AI and ML. This expertise is put to the test daily by the way the SMEs in various nations manage their operations and recognize risks and assaults based on the support systems of each nation. SMEs must examine their present condition before starting to strengthen their cybersecurity posture. We may witness new types of advancements in cybersecurity infrastructures as more businesses begin integrating AI into their cyber regimes.

The potential of artificial intelligence (AI) to improve threat detection, analysis, and response in numerous sectors may be explored in future research on cybersecurity. The effectiveness of AI-based cybersecurity

systems in defending companies and organizations from cyberattacks might be examined in this study, along with the potential and problems presented by their adoption. The project might also look at the moral ramifications of using AI in cybersecurity, including the possible dangers of prejudiced algorithms and the necessity of openness and responsibility in decision-making. In conclusion, a thorough investigation of AI-based cybersecurity may help us better understand how to use technology to raise the security and resilience of digital systems and networks.

6. **References**

1) Emer, A., Unterhofer, M., & Rauch, E. (2021). A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises. IEEE Engineering Management Review, 49(2), 98–109. https://doi.org/10.1109/emr.2021.3078077
2) Van Haastrecht, M., Ozkan, B. Y., Brinkhuis, M. J. S., & Spruit, M. A. (2021). Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics. Applied Sciences, 11(15), 6909. https://doi.org/10.3390/app11156909
3) Rawindaran, N., Jayal, A., & Prakash, E. C. (2021b). Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries. Computers, 10(11), 150. https://doi.org/10.3390/computers10110150
4) Van Haastrecht, M., Sarhan, I., Shojaifar, A., Baumgartner, L., Mallouli, W., & Spruit, M. (2021). A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs. Availability, Reliability and Security. https://doi.org/10.1145/3465481.3469199
5) Emer, A., Unterhofer, M., & Rauch, E. (2021c). A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises. IEEE Engineering Management Review, 49(2), 98–109. https://doi.org/10.1109/emr.2021.3078077
6) Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K., & Tzovaras, D. (2019). Cybersecurity in SMEs: The Smart-Home/Office Use Case. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.1109/camad.2019.8858471
7) Alahmari, A. F., & Duncan, R. a. K. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. International Conference on Electronics, Computers and Artificial Intelligence. https://doi.org/10.1109/ecai52376.2021.9515166
8) Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080
9) Alahmari, A. F., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International

Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). https://doi.org/10.1109/cybersa49311.2020.9139638

10) Onwubiko, C., & Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. Intelligence and Security Informatics. https://doi.org/10.1109/isi.2007.379479
11) Nygard, K. E., Rastogi, A., Ahsan, M., & Satyal, R. (2021). Dimensions of Cybersecurity Risk Management. Springer EBooks, 369–395. https://doi.org/10.1007/978-3-030-71381-2_17
12) Perols, R. R., & Murthy, U. S. (2021). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. Auditing-a Journal of Practice & Theory, 40(1), 73–89. https://doi.org/10.2308/ajpt-18-010
13) Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. Applied Sciences, 8(6), 898. https://doi.org/10.3390/app8060898
14) Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157
15) Wu, W., Kang, R., & Li, Z. P. (2015). Risk assessment method for cybersecurity of cyber-physical systems based on inter-dependency of vulnerabilities. Industrial Engineering and Engineering Management. https://doi.org/10.1109/ieem.2015.7385921
16) Osborn, E. (2015b). Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. ORA - Oxford University Research Archive. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e
17) Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. https://doi.org/10.3390/jcp2030027
18) Mutalib, M. M. A., Zainol, Z., & Halip, M. H. M. (2021). Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework. 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE). https://doi.org/10.1109/icraie52900.2021.9703991