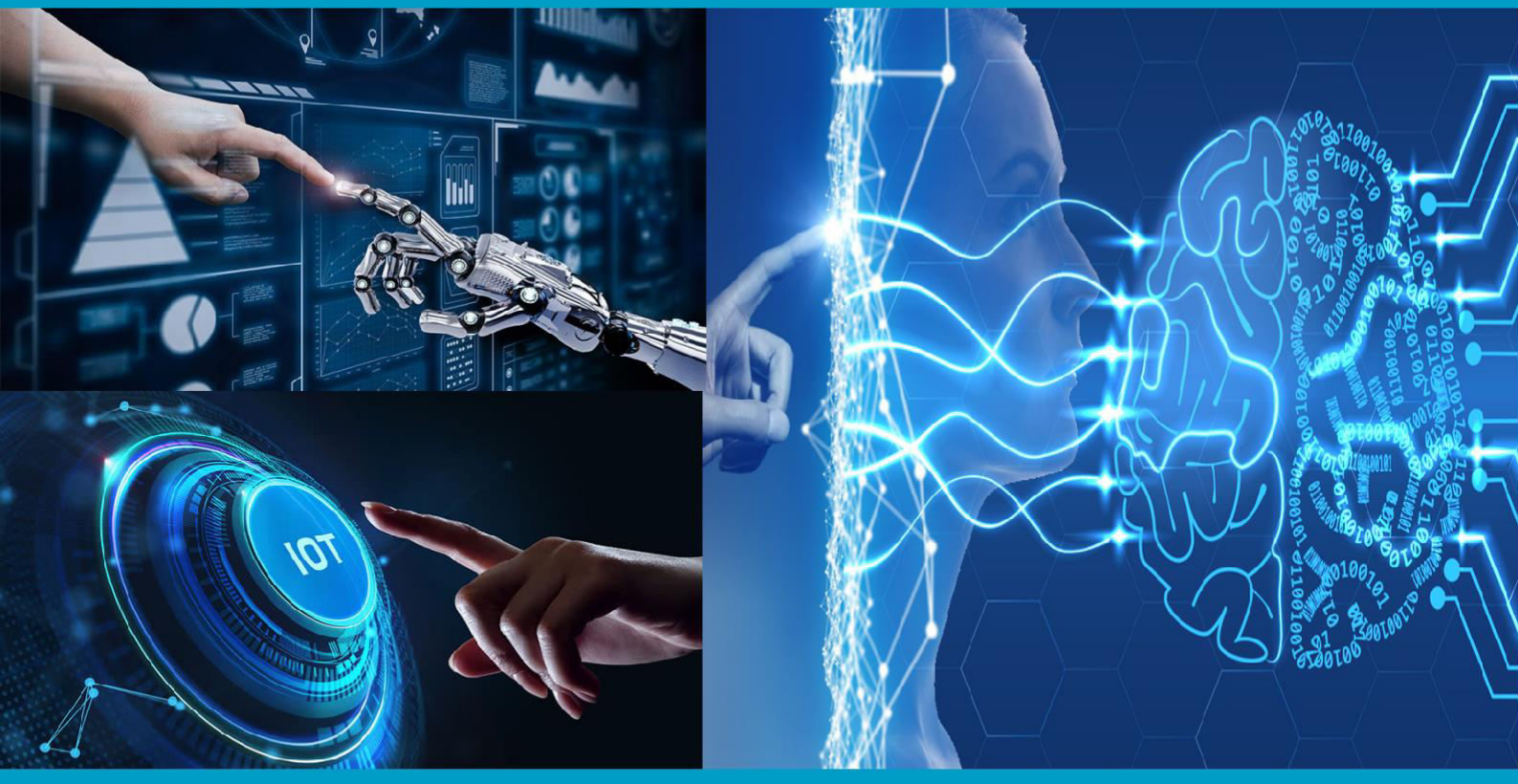
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 11, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.802

+91 99405 72462 +9163819 07438 ijmrsetm@gmail.com www.ijmrsetm.com

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

Cyber Security Issues in E-Commerce

Dr. Satya Narayan Meena

Associate Professor, EAFM, Govt. PG College, Jamwaramgarh, Jaipur, Rajasthan, India

ABSTRACT: E-commerce security threats cost online retailers billions of dollars annually and can be devastating enough to shut down online stores. Although many stores take security threats in e-commerce seriously, more can be done to protect your business and your customers from online attacks.

KEYWORDS: cyber security, E-commerce, issues, online, attacks, threats

I.INTRODUCTION

Types of Security Attacks in E-Commerce

E-commerce attacks can come in many forms that can disrupt your ecommerce platform and your customers' accounts and data. Earning the trust of your customers requires a consistent awareness of the evolving types of fraud and cyberattacks to help you ensure solutions are in place across your sales funnel.

1. Financial fraud

Financial fraud takes several forms. It involves hackers gaining access to your customer's personal information or payment information, then selling that information on the black market. It also involves fraudsters using stolen credit card information to make illegitimate purchases from your e-commerce store.

2. Phishing

Your customers are the target in a phishing scam, where a fraudster sends messages or emails pretending to be you with the goal of obtaining their private information. These messages may contain logos, URLs, and other information that appears to be legitimate, but it won't be you sending it. They'll ask customers to verify their account by logging in and then use the information to steal personal data.

3. Spamming

In an attempt to obtain personal information—or to affect your website's performance—spammers may leave infected links in their comments or messages on your website, such as on blog posts or contact forms. If you click on the links, they can take you to a spam website that exposes you to malware.[1,2,3]

4. Malware

Malware refers to malicious programs such as spyware, viruses, trojan horses, and ransomware. Hackers install it on your computer system and spread it to your customers and administrators, where it might swipe sensitive data on their systems and from your website.

5. Bad bots

People are generally aware that bots are all over the Internet, obtaining information about our habits and behaviours. Your competition, however, could use bots to gather information about your inventory and prices. They then use that information to change their prices. Or hackers can send malicious bots to e-commerce checkout pages to buy large amounts of a product and scalp it for up to 10 times the list price.

6. Distributed denial of service (DDoS) attacks

Distributed denial of service attacks happens when your servers receive an overwhelming amount of requests from various IP addresses—usually untraceable—that cause your server to crash. That means your e-commerce store isn't available to visitors, which disrupts your sales.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

7. Fake return and refund fraud

Fraudsters can obtain money from you by committing fake returns and refund fraud in many ways. Some use a stolen credit card to purchase merchandise, then claim that the card is closed and request a refund to another card. Others use counterfeit receipts to request refunds for items they haven't purchased.

8. Man-in-the-middle attacks

With technology evolving, so are hackers' schemes. Man-in-the-middle attacks allow the hacker to listen in on the communications of e-commerce website users. These users are tricked into using a public wireless network, enabling hackers to access their devices and see their browsing history. They can also access credit card information, passwords, and usernames.

E-Commerce Security Solutions

The above e-commerce security threats might be scary, but there are ways to prevent them from impacting your e-commerce marketplace. Some require fancy software, but others don't take a lot of extra work to implement. And beyond protecting your online shop, your customers will be happy that their personal data and information is kept private.

Address Verification Systems

An address verification system compares the customer's billing address against the credit card issuer's information on file. If the addresses don't match, the system prevents the transaction from going through.[4,5,6]

Stronger passwords

Many e-commerce businesses don't require their users to provide strong passwords, making client accounts easy to hack. Implement a system that requires your customers to use strong passwords with letters, numbers, and symbols to make their accounts difficult to hack into. While you're at it, make sure you and your administration have secure passwords, and ensure user access is restricted to those who need it. When employees are terminated, revoke all system access immediately.

Payment gateways

Rather than being responsible for storing and securing your clients' information, use a third party such as PayPal or Stripe to handle payment transactions separately from your website. This keeps your customers' information safer and makes you less attractive to hackers.

HTTPS

Many e-commerce businesses still use HTTP protocols, which are vulnerable to attacks. HTTPS is more secure and protects sensitive information. Before switching to HTTPS, you'll need an up-to-date SSL certification from your hosting company. It's worth it to give your customers peace of mind and protect their information—and your business.

The Importance of E-Commerce Security Best Practices

E-commerce security measures are vital to ensuring your customers' information is kept safe and preventing attacks against your business. Taking steps to safeguard your customers and your business will save you money, time, and energy in the long run. It might even protect your reputation.

American Express customers enjoy a number of security features and fraud protection services to protect every transaction for both merchants and Cardmembers.

With American Express SafeKey, every point-of-sale and online purchase is verified, meaning you won’t be held liable for fraudulent purchases. From your customer’s perspective, our fraud detection and identity verification are seamlessly implemented within your e-commerce platform, ensuring that customers don’t abandon their purchases during transaction verification.

You can also speak to your American Express merchant representative to understand how our Enhanced Authorization services can provide immediate transaction verification by leveraging our Global Merchant Network.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

Whether your point-of-sale is a contactless in-store card reader or an online e-commerce platform, purchases made with American Express Cards provide your customers with a frictionless experience and your business with the security of knowing every purchase is valid.[7,8,9]

II.DISCUSSION

As organizations transition to the digital age, the danger of cyberattacks increases. This is because users frequently disregard good cyber hygiene.A compromise in internet security may have significant consequences for both customers and organizations. As an e-commerce business owner, you only have one chance to get your e-commerce security right.If your online business loses critical information due to e-commerce security concerns, you will almost certainly lose many potential clients.

For instance, clients would lose their trust in the company, and the business would gain a bad reputation.Typically, hackers target e-commerce store administrators, users, and workers using various malware evasion techniques.Securing cyber assets means having adequate protection for e-commerce security concerns.

Basic e-commerce security

Building e-commerce security consists of protocols safeguarding people who engage in online transactions.You must earn your client's trust by implementing these e-commerce security basics:

Privacy

Privacy is the practice of restricting the sharing of consumer data with unauthorized third parties.This means no one else should have access to a customer's personal information or account data besides the online retailer they have chosen.When sellers allow outsiders access to such information, a breach of confidentiality occurs.E-commerce should implement anti-virus, firewall, encryption, and other data security measures.

Integrity

Another critical element in e-commerce security is integrity. The idea stipulates that the online business uses the information provided by the clients precisely as it is.It entails ensuring that any information given by clients online remains unmodified.So any change to the data leads the customer to lose trust in the business's security and integrity.

Authentication

This concept of e-commerce security demands that both the supplier and the buyer be genuine. They should be who they claim to be.The company should demonstrate that it is authentic, sells tangible goods or services, and has a legitimate claim about the products.Clients should also provide evidence of identification for the seller to feel confident about online transactions.

Non-repudiation

Non-repudiation is a legal concept that urges participants in a transaction not to deny their acts.This means that the company and the buyer must complete the deal they began and should finish the transaction as it is.As a result, a party in that transaction cannot refuse a signature, email, or purchase.

8 e-commerce security issues

Building a well-rounded website is excellent, but your customer's information could be vulnerable to hackers without proper security.There are guidelines and best practices to follow to help ensure you're doing everything you can to keep your online environment secure.But first, let's look at the most significant e-commerce security issues:

1. Malware and website hacking

Malicious hackers use malware to access users' data on online shopping websites.Malware and website hacking is dangerous. Malware can be a severe threat to your business and website.Hackers use malware to steal user data from the client's side or reroute them through sending malicious code or affiliate links, which will cost the owner of the website some loss.Every online merchant should be aware of this advanced method of an e-commerce security issue and the risk of having their websites hacked.[10,11,12]

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

2. Payment processing issues

The payment processing issue is a new e-commerce threat cybercriminals use.Fraudulent merchants capture clients' payment information through a gateway, while legitimate merchants implement payment processing correctly.This issue also occurs when data is stolen or altered without the user's knowledge which can later become identity theft.

3. Credit card skimming

Credit card skimming as an e-commerce security issue is a very dangerous activity affecting the financial and sensitive data of both businesses and clients.Anyone who has ever handed a stranger their credit card knows how easy it is for a shop assistant to copy their essential information.Because of this, malicious hackers can steal credit card details from online payment systems and even from ATMs by taking the receipts left by customers.

4. Third-party vendor issues

By storing payment information with a third-party vendor, businesses risk getting hacked. Hackers can infiltrate third-party websites or accounts.They'll be granted access to a website through the portal of one or more third parties.For example, when an attacker breaks into an ad-serving service of your e-commerce site, the hacker now has access to the stats pages, cookie store, and all of the ads on your site.

5. Unauthorized employee access

Unauthorized access by certain employees can result in illegal purposes like reading emails, deleting data, and damaging or stealing information.When unauthorized employees gain access to confidential files and personal accounts, they can make an unauthorized purchase on behalf of the company.It also reveals that in most situations, the high risk associated with this e-commerce security issue is a financial loss.

6. Sensitive data exposure

Sensitive data exposure, also known as a data breach, can be very dangerous for data security and operations.This happens when hackers gain access to a website's databases and steal sensitive data, like credit card and Social Security information, for financial gain.

7. Insufficient transaction security

Insufficient transaction security occurs when thieves find ways to steal money through unauthorized transactions between accounts.E-commerce transaction security problems often result from poor digital certificate encryption performance. This causes personal information leakage and digital certificate data modification attacks.

8. Lack of PCI compliance

The lack of PCI compliance can lead to neglecting IT security audits and prevent keeping data secure and safe.The organization's financial details and even a customer's credit card details can be at risk when the system gets hacked without encryption.

Essential tips to avoid e-commerce security issues

E-commerce security is an important aspect of the online shopping experience.For many businesses, adequate security measures are often a low priority that gets assigned to the bottom of their list of things to do.However, if you're aware of these issues, you can do what it takes to ensure you don't fall victim to the latest scams.So if you are thinking of setting up an online shop or an e-commerce website, here are some tips to avoid e-commerce security issues:

Use the latest web browser

Using an old browser version can make your e-commerce website vulnerable to hackers. So update your web browser whenever a new version is available.Many free online services allow you to check for updates immediately. Remember to do it frequently, as running an outdated browser puts you at significant risk.The newest version will have all the latest security fixes, which can prevent online attacks.[13,14,15]

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

Always log out after shopping online

You can never be sure that someone isn't watching the cookies on your browser and gaining access to your account.There have been increased phishing attacks to steal customers' credit card information and other personal information like passwords.Various online forums have discussed the same thing, which is why we need to take an extra step to be sure that hackers are not using our login details.One way of doing this is simply logging out of your account after shopping on e-commerce websites and never leaving your browser window open on non-secure sites.

Shop with reputable merchants

The web is full of shopping cart plugins. They all have extensions, features, and lots of information to make you buy.But what makes you choose one over the other? It takes much more than just fancy features to help you make the right choice.You should only shop with reputable merchants who adhere to the latest industry standards to provide an outstanding buying experience and security.

Investigate third-party providers

Investigate third-party providers because there's no guarantee of their capabilities, efficiency, or quality yet, and you still need to know who they are.This often means there is a chance of your data not being appropriately encrypted, which can result in security breaches.If you have an e-commerce website, you must check out third-party websites and try to find any security issues.

Ensure your site has an SSL certificate

It's necessary to use an SSL certificate for e-commerce websites or anywhere where there is a transaction involved.A Secure Socket Layer (SSL) certificate is an encrypted link between the user and your server, and SSL monitoring checks for its validity.The SSL security encrypts the data transferred from the server to the client and the data on your server.This keeps your customer's private information, such as their credit card number and address, from being stolen by hackers.When encryption is applied to data in motion, such as through email or instant messaging, unauthorized parties can't access it.

Only accept secure transactions

From attackers to bots, online criminals are always looking for cracks in your armor.That's why it is vital to offer your customers a safe environment when paying for purchases on your site.A specific payment transaction allows the processor to encrypt sensitive customer data, such as account and card details while transmitting information to the bank.

Set up fraud alerts

Setting up fraud alerts is essential if you have a credit card or debit card online.This will ensure that if someone tries to take a payment from your account without your permission, you'll know about it immediately.You can also set up alerts depending on how you buy something online. For example, if you're purchasing goods from an individual, you can set up an alert for each item.

Avoid public Wi-Fi

Using public Wi-Fi is risky because most hackers use it to access private and personal data. It leaves you vulnerable to stolen sensitive information such as usernames, passwords, and credit card information.If you are transacting to an online store, it would be best to use your mobile data or private Wi-Fi to ensure that you are keeping your information secure.

Only store the necessary information

It is important only to store the minimum amount of information required to complete your online purchase.By keeping what you only need, you will have a little information on a page, making it difficult for hackers to extract information quickly.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

Avoid these e-commerce security threats by following these tips

Any personal data you collect will be compromised at some point. But what matters most is how prepared you are to manage any cyber risks.Being a wise e-commerce merchant means taking every precaution to keep yourself, your business, and your customers safe.E-commerce merchants who know how to avoid ecommerce security threats can effectively secure their business, customers' information, and products from cyberattacks.Follow and adopt these essential tips; your e-commerce site should be secure enough to withstand serious cybersecurity threats.[16,17,18]

III.RESULTS

Protecting E-Commerce Businesses from Cyber Threats

E-commerce businesses constantly increase their staffing and spending to bolster their information security. Unfortunately, cybercriminals also invest in identifying vulnerabilities and finding new ways to exploit them. Consequently, the frequency and sophistication of cyber attacks have increased dramatically in recent years.

Any business offering e-commerce capability to its customers in the current cyber threat landscape must implement effective e-commerce security to stay ahead of potential security breaches.

Combining best cybersecurity practices and solutions tailored to e-commerce is key to providing a robust defense against cybercriminals. Here are the things to focus on to protect an e-commerce business.

Compliance Risks

Depending on the industry, e-commerce businesses may be subject to various regulations and compliance standards. Failing to meet compliance standards can result in significant fines or penalties, especially if a data breach occurs due to compliance failure.

Get PCI DSS Certified

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of data security standards defined by the Payment Card Industry Security Standards Council (PCI SSC). This global forum includes American Express, Mastercard, and Visa.

The standards apply to any business that manages credit card transactions, which includes the majority of e-commerce businesses. The standards set out minimum security requirements to protect customer credit card information.

While PCI-DSS is not a law, it is mandated by the contracts of the major card payment brands. Non-compliance with the security standard can result in severe penalties, including a monthly fine of between $5000 and $100,000, plus penalties from the acquiring bank.[19,20,21]

Get GDPR Ready

Unlike PCI DSS, the General Data Protection Regulation (GDPR) is a law governing EU countries. Since 2018, the European Union (EU) privacy law has applied to any organization that targets or collects data about EU citizens.

Ensuring GDPR compliance is an excellent way to protect a business from cyber risks associated with e-commerce. GDPR's primary principles include the following:

- Data minimization
- Storage limitation
- Data integrity and confidentiality

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

Under GDPR, organizations must collect as little data as necessary, store it for only as long as needed, and protect it with the latest security. Following each principle contributes to an organization's security posture, boosting information security.

Network and Data Security Practices

Here is a short list of the best network and data security practices businesses can follow to improve their cybersecurity quickly:

Attain SSL/TSL Certificates

HTTPS is a network protocol that encrypts and verifies transmissions, making it much more secure than HTTP. Online businesses that process sensitive data, including financial information, should always use HTTPS to offer higher security to their users.

To implement HTTPS hosting, also known as Secure Socket Layer (SSL) or Transport Layer Security (TLS), a website requires an SSL certificate, which is code that enables encrypted connections.

With the implementation of HTTPS, hackers will find it far more difficult to intercept, read, or modify transmitted data, adding another layer of protection for businesses and their customers.

Use Multi-Factor Authentication (MFA)

With multi-factor authentication, users must provide at least two ways of proving their identity before accessing their account. In addition to a username and password combination, MFA demands further authentication, such as a one-time PIN, identity verification via an app on a mobile device, answering a security question, or performing a biometric scan.

MFA can prevent many data breaches, so organizations should ensure their staff uses it and encourage their customers to do the same. While it can seem burdensome because it is more time-consuming, it is far more secure than using passwords alone and far less time-consuming than mitigating a successful data breach.

Implement Strong Passwords

Many data breaches occur because of weak access credentials. Therefore, organizations should encourage using strong passwords and good password hygiene for their customers and staff.

A strong password must be at least eight characters long and contain a combination of upper and lowercase letters, numbers, and symbols. Furthermore, users should not re-use the password for another site. To achieve secure, efficient password management, using a password manager app can be useful to keep passwords strong, unique, and regularly updated.

Installing Anti-Malware, Antivirus, and Firewalls

Businesses can implement low-cost software such as anti-malware, antivirus, and firewall technology to provide baseline defenses against external threats.

The latest device protection systems include AI and machine-learning technology, providing continuous monitoring and real-time threat detection, which can be invaluable in thwarting cybercriminals' attempts to access confidential customer data and make fraudulent transactions.

Businesses can take their protection further by maintaining firewalls to monitor and filter all traffic attempts to enter or leave the network. A firewall is an essential network security measure, as it will help prevent confidential information

from leaving the network without people knowing, log user activity, and prevent modification of data by hackers or malicious software.

Update Hardware and Software

All devices and software applications should be updated regularly to avoid being exploited by vulnerabilities. Unpatched hardware and software may not be equipped to defend against the latest threats and vulnerabilities.[20,21,22]

Most updates from software developers are related to security. Regularly checking for and installing updates provides potentially vital security patches, fixing vulnerabilities that cybercriminals could otherwise exploit.

Third-Party Risk Management

E-commerce businesses also need to take charge of third-party risks. A business's attack surface is not limited to the company. Its cloud-service providers, suppliers, and business partners are all potential weaknesses in the supply chain.

Businesses need to see, understand, monitor, and remediate third-party risk, especially when many online retailers rely on multiple third-party plugins for the functionality of their stores. However, as businesses scale, this can be a challenging task to complete, especially when hundreds or thousands of vendors and suppliers are involved. Businesses can use solutions such as UpGuard Vendor Risk to help manage their third and fourth-party risks.

Cybersecurity Awareness and Training

Human error is often the first entry point in many data breaches. To create a strong defense against cybercrime, retailers should implement cybersecurity training for all employees. Furthermore, different groups should receive different training according to their risk exposure.

A longer-term solution is to develop a cybersecurity culture. This goes beyond cybersecurity training because it begins with increasing awareness and authentic engagement with cybersecurity strategy at the board level and then having this filter down throughout the company.

To disseminate the cybersecurity culture, the C-suite should employ various techniques, including internal campaigns with consistent messaging, regular cybersecurity updates in meetings, incentives for cybersecurity engagement, and simulations and drills.

In an organization with a mature cybersecurity culture, the staff is more likely and be able to identify, report, and remediate suspicious activity and behavior.

Access Control

Access control protects sensitive information by determining who can access certain information and resources. This reduces the attack surface since not everyone in the business can access personal data.

An access control system will also help an organization contain malicious software or identify the source of a data leak or breach because it limits the pathways a cybercriminal can use to access the system.

Network Segmentation

Confidential data should be kept separate from other information on the network. This can be achieved via network segmentation, with personal customer information firewalled and monitored to reduce the risk of a data breach or the spread of malware from other parts of the network.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

By segmenting networks, it prevents lateral movement from both internal parties and cybercriminals attempting to gain unauthorized access.

Data Backups

Ideally, businesses will avoid data breaches and critical cyber incidents that disrupt business operations. However, having backups is essential when things don't go the way of the organization. A backup system can help a business become operational faster after an incident and mitigate the impact of data theft.

Backups must be performed regularly to ensure the data is relevant and can keep the business functional during a critical incident. The backup should be stored away from the primary networks, such as with a secure cloud storage service provider, to ensure that the network incident doesn't also affect the backup.

IV.CONCLUSION

Incident Response Plan

Businesses with incident response plans spend less time and money attempting to resolve data breaches compared to unprepared firms. A documented incident response plan gives stakeholders a clear guide to help them coordinate what happens after a cyber incident. Responding quickly to a cyber incident can help a business save money and its reputation.

The incident response plan needs to be checked regularly to ensure that contact details and roles and responsibilities are up to date. It also needs to reflect the current information security policy (ISP) to ensure an efficient and effective response to cyber incidents.[22]

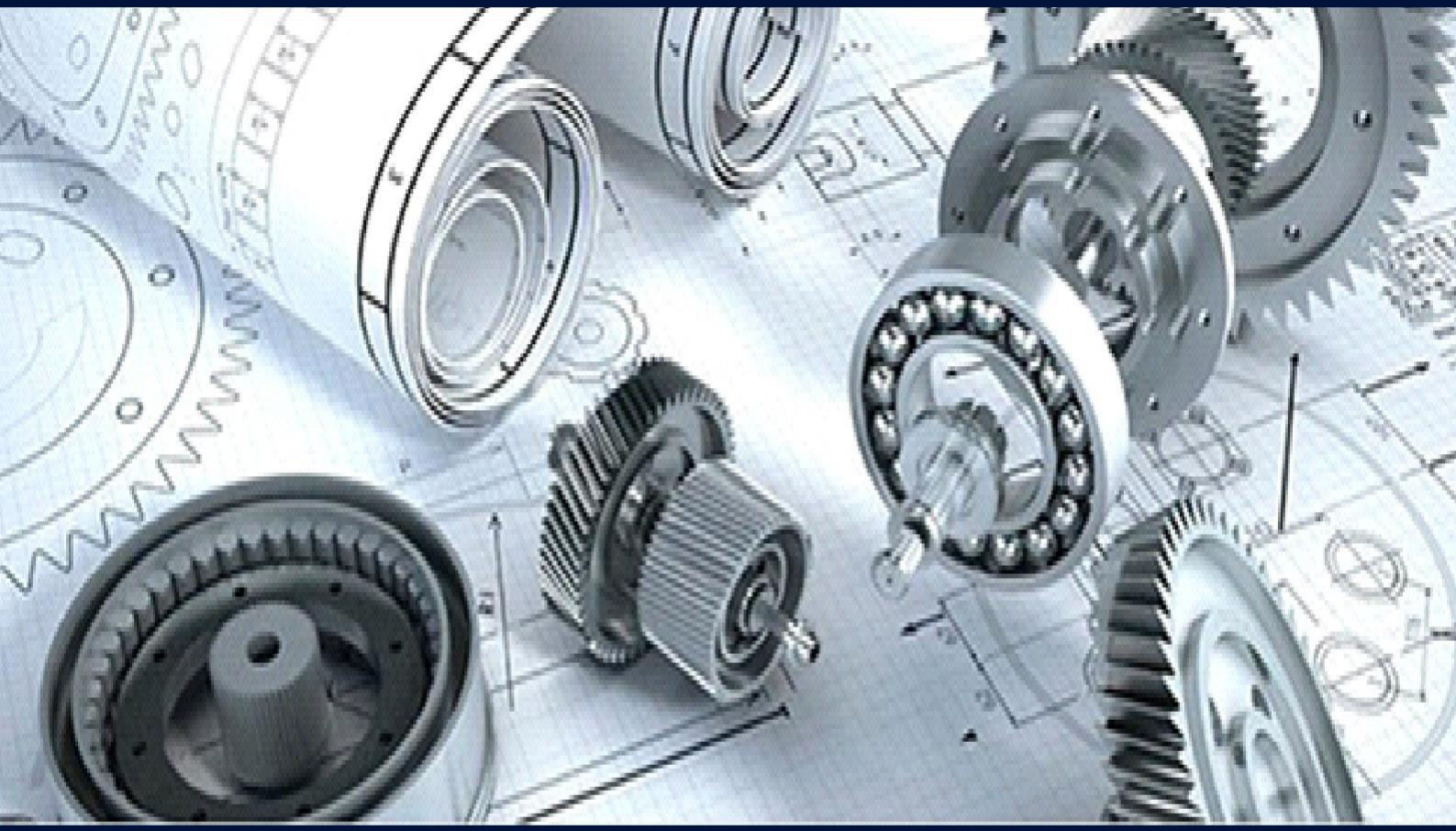
REFERENCES

1. ^ "A chronology of data breaches reported since the ChoicePoint incident." (2005). Retrieved October 13, 2005.
2. ^ "Electronic privacy information center bill track: Tracking privacy, speech and civil liberties in the 109th congress." (2005). Retrieved October 23, 2005.
3. ^ "How computer viruses work." (2005). Retrieved October 10, 2005.
4. ^ "The National Strategy to Secure Cyberspace Archived 2012-02-27 at the Wayback Machine." (2003). Retrieved December 14, 2005.
5. ^ "Notice of security breach – civil code sections 1798.29 and 1798.82 – 1798.84." 2003). Retrieved October 23, 2005.
6. ^ "Richard Clarke interview." (2003). Retrieved December 4, 2005.
7. ^ Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Richardson, R. (2005). "2005 CSI/FBI computer crime and security survey." Retrieved October 10, 2005.
8. ^ Heiman, B. J. (2003). Cybersecurity regulation is here. RSA security conference, Washington, D.C. Retrieved October 17, 2005.
9. ^ Kirby, C. (2003, December 4, 2003). "Forum focuses on cybersecurity". San Francisco Chronicle.
10. ^ Lemos, R. (2003). "Bush unveils final cybersecurity plan." Retrieved December 4, 2005.
11. ^ Menn, J. (2002, January 14, 2002). "Security flaws may be pitfall for Microsoft". Los Angeles Times, pp. C1.
12. ^ Rasmussen, M., & Brown, A. (2004). "California Law Establishes Duty of Care for Information Security." Retrieved October 31, 2005.
13. ^ Schmitt, E., Charron, C., Anderson, E., & Joseph, J. (2004). "What Proposed Data Laws Will Mean for Marketers." Retrieved October 31, 2005.
14. ^ Jennifer Rizzo. (August 2, 2012) "Cybersecurity bill fails in Senate." Accessed August 29, 2012.
15. ^ Paul Rosenzweig. (July 23, 2012) "Cybersecurity Act of 2012: Revised Cyber Bill Still Has Problems." The Heritage Foundation. Accessed August 20, 2012.
16. ^ Ed O'Keefe & Ellen Nakashima. (August 2, 2012) "Cybersecurity bill fails in Senate." The Washington Post. Accessed August 20, 2012.
17. ^ Alex Fitzpatrick. (July 20, 2012) "Obama Gives Thumbs-Up to New Cybersecurity Bill." Mashable. Accessed August 29, 2012.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.802| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 11, Issue 4, April 2024 |

18. ^ Brendan Sasso. (August 4, 2012) "After defeat of Senate cybersecurity bill, Obama weighs executive-order option". The Hill. Accessed August 20, 2012.
19. ^ Jaikumar Vijayan. (August 16, 2012) "No partisan fight over cybersecurity bill, GOP senator says". Computerworld. Accessed August 29, 2012.
20. ^ Carl Franzen. (August 2, 2012) "As Cybersecurity Bill Fails In Senate, Privacy Advocates Rejoice". TPM. August 29, 2012.
21. ^ Alex Fitzpatrick. (August 2, 2012) "Cybersecurity Bill Stalls in the Senate". Mashable. Accessed August 29, 2012.
22. ^ Jody Westby (August 13, 2012) "Congress Needs to Go Back To School on Cyber Legislation". Forbes. Accessed August 20, 2012.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com