Impact of Cyber Security in Economy

Aarcha SS
Assistant Professor, Department of Commerce, S.N. College, Kollam

ABSTRACT

Cyber security specify the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. Computer security, cyber security or information technology security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.Digital marketing has introduced a whole new world of advertising opportunities for businesses of all sizes. However, the way it works has opened much more space for a particular kind of threat that can seriously damage our brand. Marketing can also undermine online security efforts by disseminating outdated, or outright false security-related information, promoting software with serious security flaws, as well as encouraging the risky online behavior. In other words, cyber security should be a top concern among digital marketers.

KEY WORDS: Cyber security, Cloud security, Digital marketing.

INTRODUCTION

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to

ISBN: 978-81-955611-3-1

other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

CHALLENGES OF CYBER SECURITY

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

MANAGING CYBER SECURITY

The National Cyber Security Alliance, through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across all business

ISBN: 978-81-955611-3-1

practices. NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information; and outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others. Following a cyber risk assessment, develop and implement a plan to mitigate cyber risk, protect the "crown jewels" outlined in your assessment, and effectively detect and respond to security incidents. This plan should encompass both the processes and technologies required to build a mature cyber security program. An ever-evolving field, cyber security best practices must evolve to accommodate the increasingly sophisticated attacks carried out by attackers. Combining sound cyber security measures with an educated and security-minded employee base provides the best defence against cyber criminals attempting to gain access to your company's sensitive data. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application **security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

ISBN: 978-81-955611-3-1

· **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

● End-**user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

TYPES OF CYBER THREATS

The threats countered by cyber-security are three-fold:

1. **Cyber crime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyber terrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

● **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

• **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

● **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could

ISBN: 978-81-955611-3-1

capture credit card details.

- **Ransom ware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL INJECTION

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a data based via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack . This malicious campaign affected the public, government,

ISBN: 978-81-955611-3-1

infrastructure and business worldwide.Dridex is a financial Trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions. In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.

is a sophisticated Trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

End-user protection

Emotet End-user protection or endpoint security is a crucial aspect of cyber security. After all, it is often an individual (the end-user) who accidentally uploads malware or another form of cyber threat to their desktop, laptop or mobile device.

So, how do cyber-security measures protect end users and systems? First, cyber-security relies on cryptographic protocols to encrypt emails, files, and other critical data. This not only protects information in transit, but also guards against loss or theft.

In addition, end-user security software scans computers for pieces of malicious code, quarantines this code, and then removes it from the machine. Security programs can even detect and remove malicious code hidden in Master Boot Record (MBR) and are designed to encrypt or wipe data from computer's hard drive.

Electronic security protocols also focus on real-time malware detection .

ISBN: 978-81-955611-3-1

Many use heuristic and behavioural analysis to monitor the behaviour of a program and its code to defend against viruses or Trojans that change their shape with each execution (polymorphic and metamorphic malware). Security programs can confine potentially malicious programs to a virtual bubble separate from a user's network to analyse their behaviour and learn how to better detect new infections.

Security programs continue to evolve new defences as cyber-security professionals identify new threats and new ways to combat them. To make the most of end-user security software, employees need to be educated about how to use it. Crucially, keeping it running and updating it frequently ensures that it can protect users against the latest cyber threats.

CYBER SAFETY TIPS - PROTECT YOURSELF AGAINST CYBERATTACKS

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1. **Update your software and operating system:** This means you benefit from the latest security patches.
2. **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
3. **Use strong passwords:** Ensure your passwords are not easily guessable.
4. **Do not open email attachments from unknown senders:** These could be infected with malware.
5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.
6. **Avoid using unsecure Wi-Fi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

HOW THE BUSINESS CAN BENEFIT FROM A CYBER SECURITY SOLUTION

1. **It Can Protect Your Business** – The biggest advantage is that the best in IT security cyber security solutions can provide comprehensive digital protection to your business. This will allow your employees to surf the internet as and when they need, and ensure that they aren't at risk from potential threats.
2. **Protects Personal Info** – One of the most valuable commodities in the digital age is personal information. If a virus is able to obtain personal information regarding your employees or customers, they

ISBN: 978-81-955611-3-1

are quite capable of selling that information on, or even using it to steal their money.

3. **Allows Employees to Work Safely** – Without the best cyber security solutions for your business, you and your employees are constantly at risk from a potential cyber-attack. If your system, or even individual computers, become infected than that can really hamper their productivity and even force you to replace computers.
4. **Protects Productivity** – Viruses can slow down personal computers to a crawl, and make working on them practically impossible. This can cause a lot of wasted time for your employees, and can often bring your entire business to a standstill.
5. **Stop Your Website from Going Down** – As a business, the chances are you're hosting your own website. If your system becomes infected, there is a very real chance that your website be forced to shut down. This means that not only will you be losing money from missed transactions, but you will also lose customer trust and certain viruses can often do lasting damage to a system.
6. **Denies Spyware** – Spyware is a form of cyber infection which is designed to spy on your computer actions, and relay that information back to the cyber-criminal. A great cyber security solution, such as 'Fortinets Fort iGATE firewall, can prevent this spyware from taking effect and ensure that your employees' actions remain private and confidential within your workplace.
7. **Prevents Adware** – Adware is a form of computer virus which fills your computer with advertisements and is fairly common. However, all these adverts can really have an impact on productivity and can often allow other viruses to enter your computer once you've accidentally clicked on them.
8. **A Consolidated Solution** – The very best kinds of IT security for your business will offer a comprehensive solution to protect against a diverse range of issues. Ideally, your security needs to include a firewall, anti-virus, anti-spam, wireless security and online content filtration.
9. **Support Your IT Expert** – It might be unpleasant to hear, but most cyber-criminals will have much more experience than your average employee when it comes to digital crime. The best IT security systems can provide your team with the features and support that

ISBN: 978-81-955611-3-1

they need to effectively fight against even the most determined criminal.

10. **Inspire Confidence in Your Customers!**– If you can prove that your business is effectively protected against all kinds of cyber threats, you can inspire trust in your customers and clients. They will then feel more confident when purchasing your products or using of your services.

CONCLUSION

Every online enterprise has to contend with the possibility of a security breach somewhere down the line, and this includes businesses specializing in digital marketing. Another security issue related to digital marketing is the fact that it reaches a broad audience. Sharing a link to a website that hosts malware is much more devastating when it is done through a trusted online source, such as a Twitter account managed by a marketing firm. Marketing can also undermine online security efforts by disseminating outdated, or outright false security-related information, promoting software with serious security flaws, as well as encouraging the risky online behaviour. In other words, cyber security should be a top concern among digital marketers. Neglecting can have drastic consequences on everything from the marketing company's bottom line, to unsatisfied clients, to endangering the online public at large.The inherent social sharing aspect found across all social media channels makes it difficult for any business to completely safeguard itself against security challenges. But with that said, fostering a security-aware culture ensures businesses are mindful of such security risks. Digital marketers must be educated and informed of the potential security risks inherent with the use of any social platform.

REFERENCES

1. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518,
2. Von Solms, Rossouw, Johan Van Niekerk. From information security tocyber security. Computers and Security. 2013; 38: 97–102
3. Data Warehousing and Data Mining Techniques for Cyber Security by Anoop Singhal.
4. Preeti Aggarwal “Application of Data Mining Techniques for Information Security in a Cloud: A Survey” in International Journal of Computer Applications (0975 – 8887) Volume 80 No 13, October 2013.

ISBN: 978-81-955611-3-1