The Evolution of IT Security in the Last 30 Years

Benjamin O Ugwu

Atlantis University, Miami Florida USA

Abstract

This project is on the evolution of IT security (Information Technology Security) in the last 30 years – since the time of mainframe. The goal of this project is to present an indepth history of how information security has evolved over the last thirty (30) years. It starts by discussing the concept and meaning of IT security, its related terms, the need for IT security, different types of IT security, and how it impacts us as individuals, organizations or businesses. It goes on to discuss the series of events that have led to the different developments and innovations in the strategies employed in IT security today. It discusses encryption technology which has provided us with a secure way of information exchange, using a Python programming language code to demonstrate encryption in action. It ends with a conclusion, offering suggestions on how best to handle present and future challenges that IT security faces. This project aims to help us see how far we have come in the field of IT security over the years, mistakes made, lessons learned and how best to tackle the challenges IT security faces today and might face in the future as a way forward.

Keywords: IT Security, Information Security, Cybersecurity, Encryption, Mainframe.

Table of Contents

The Evolution of IT Security in the Last 30 Years

Today, the issue of IT security has become a top issue on just about the minds of everyone, especially corporations. However, this was not always so since security did not occur to the close-knit crew of academic researchers who trusted each other in the use of computers and the networks involved (Tim, M. 2019).

With today's pervasive use of the internet, the proliferation of mobile devices, major technology trends such as the Internet of Things (IoT), and cloud computing, we have witnessed a modern surge in data breaches and cyberattacks and the subject of IT security can no longer be ignored.

Protecting the security and privacy of data in computer networks and systems has become a major challenge in the modern computer age. As organizations embrace the cloud and mobile computing to connect with their customers and optimize their business operations, they take on new risks. Traditional IT boundaries have disappeared, and hackers have many new attack vectors. It should, therefore, come as no surprise that IT security is one of the biggest threats organizations of all shapes and sizes face today.

There were allegedly 918 data breaches compromising nearly 2 billion data records in just the first six months of 2017. Compared to the last six months of 2016, the number of stolen, lost, or compromised records increased by an astounding 164%. Of the 918 data breaches, over 500 (59% of all breaches) had an unknown or unaccounted number of compromised data records (Gemalto, 2017).

Looking at just the financial impact of cybercrimes, the 2017 average annualized cost of cybersecurity per enterprise was $11.7 million, which represents a 22.7 percent increase over the prior year, 2016. The same survey reports that the cost of cybercrimes tops $17 million per year for organizations in industries such as financial services, utilities, and energy.

With the constantly evolving and dynamic campaign strategies cybercriminals are adopting such as ransomware-as-a-service, it's no surprise that 87 percent of board members and C-level executives (such as CEO (Chief Executive Officer), COO (Chief Operating Officer), CFO (Chief Financial Officer), CIO (Chief Information Officer)) state that they lack confidence in their organization's level of cybersecurity preparedness (Morgan, 2019).

The impact of a Security breach incidence may range from costing an organization its reputation, loss of huge sums of money (please see Figure 9. Global Average Total Cost of a Data Breach (IBM, 2019) in Appendix A), to a complete shutdown of the business. According to Robert (2019), 60 percent of small companies go out of business within six months of falling victim to a data breach or cyber-attack.

Unfortunately, Data breaches happen daily, in too many places at once to keep count (Taylor, A., 2018). The number of security breaches disclosed yearly continue to grow (please see Figure 10. Number of Cybersecurity Breaches Disclosed per Year (Audit Analytics, 2019) in Appendix A). There is no organization, be it a Fortune 500 company or a small business, that is beyond the reach of today's malicious and sophisticated hacker.

The good news is; one can say that these attacks all have one thing in common, which is IT security issues. Therefore, by tackling IT security issues in the right way, the risks of these attacks could be significantly diminished.

This project is essential in the field of risks and information system control as it would act as a reference on how far we have come in the field of IT security over the years with a focus on the last thirty (30) years, presenting past security mistakes, how they have shaped IT security today and proffer innovative recommendations that would improve IT security now and in the future.

Literature Review

What is IT security?

IT security (Information Technology Security) could be referred to as a set of strategies employed to prevent unauthorized access to organizational assets such as computers, data, and networks. It maintains the confidentiality, integrity, and availability of sensitive information.

It is sometimes referred to as cybersecurity or information security. While cybersecurity is mostly used to refer to security involving the internet, information security is sometimes used to refer to logical security (security of data excluding physical security).

Information security could, therefore, be defined as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information. Information security includes the areas of information security management, data security, and network security (Michael & Herbert, 2018).

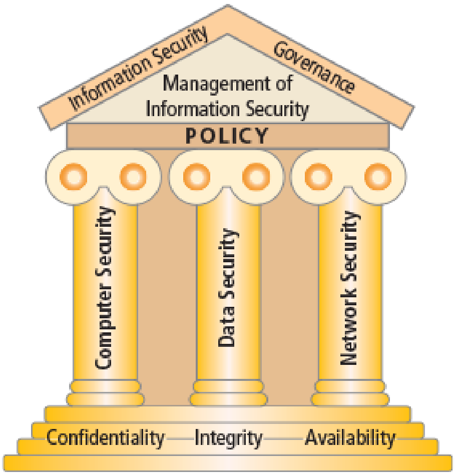


Figure 1. Components of Information Security (Michael, E. W., & Herbert, J.M., 2018)

Cryptography

Cryptography or cryptology is the practice and study of techniques for secure communication such as Encryption (a two-way function that includes encryption and decryption- achieved through encryption algorithms and keys) and Hashing (a one-way function that changes a plain text to a unique digest that is irreversible – achieved using hash functions).

The word "cryptography" is a combination of the Greek words for "secret" and "writing". The cryptographic technique of encryption is the bedrock of modern information security and will be discussed below.

Encryption

Encryption could be described as the process of converting an original message (plaintext) into a form that cannot be used by unauthorized individuals (ciphertext).

The main purpose of encryption is to protect the confidentiality of digital data or information stored on computer systems or transmitted over the public internet or any other computer network such as local area networks. Encryption makes many of our modern technological security marvels possible. Every time we make a mobile phone call, buy something with a credit card in a shop or on the web, or even get cash from an ATM (Automated Teller Machine), encryption bestows upon those transactions the confidentiality and security to make them possible and secure.

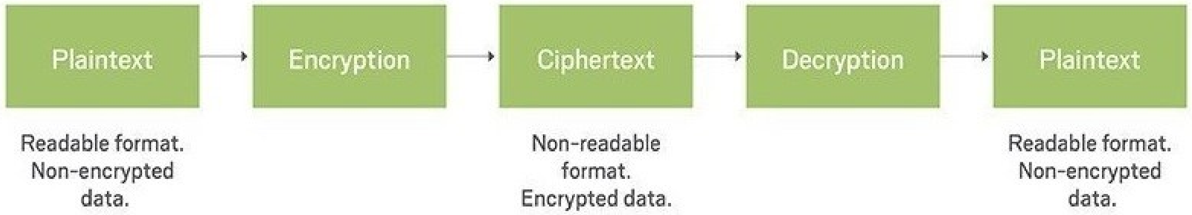

Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

Figure 2. Cryptography Process (Margaret, R., 2018)

Encryption is achieved through cryptographic algorithms, which scramble the message so no-one else can read it except its intended recipient, thereby protecting our information against prying eyes. There are two types of encryption which are Symmetric and asymmetric encryption,

Symmetric and Asymmetric encryption are two group categories of cryptographic algorithms. Cryptographic algorithms are referred to as the mathematical formulas or methods which are used to convert an unencrypted message (plaintext or cleartext) into an encrypted message (ciphertext or cryptogram). They are sometimes also referred to as the programs that enable the cryptographic processes of encryption (converting plaintext to ciphertext) and decryption (converting ciphertext to plaintext).

Another information is used in conjunction with cryptographic algorithms to create cyphertext, this information is called key or cryptovariable. The strength of many encryption applications, algorithms and cryptosystems is measured by key size (measured in number of bits). The length of the key increases the number of random guesses and time required to break the code and decrypt the ciphertext. Therefore, the longer the key size, the greater the strength of the encryption.

The fundamental difference between symmetric and asymmetric encryption is based on the types of keys they use for encryption and decryption operations.

The operation of Encryption algorithms or methodologies that require the same key (a single secret key) to encrypt or encipher and decrypt or decipher the message are called private-key encryption or symmetric encryption. While those that require two different keys (private and public keys) are called public-key encryption or asymmetric encryption. The private key is kept secret (just like the key in symmetric encryption) and is known only to the owner of the key pair (private-public key pair) for decryption. The public key is stored in a public location where anyone can use it for encryption of messages going to the public key owner. Thus the public key is made public.

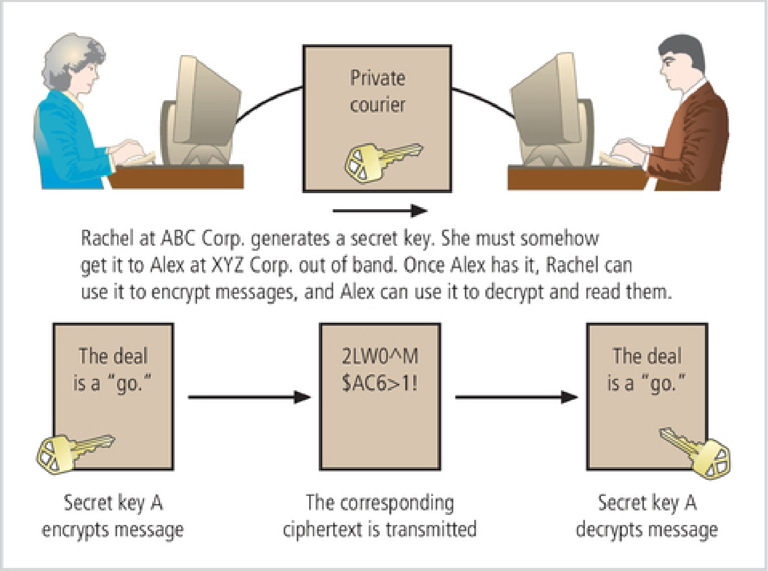

Private courier
Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out of band. Once Alex has it, Rachel can use it to encrypt messages, and Alex can use it to decrypt and read them.
The deal is a "go."
2LW0^M $AC6>1!
The deal is a "go."
Secret key A encrypts message
The corresponding ciphertext is transmitted
Secret key A decrypts message

Figure 3. Example of Symmetric Encryption (Michael, E. W., & Herbert, J.M., 2018)

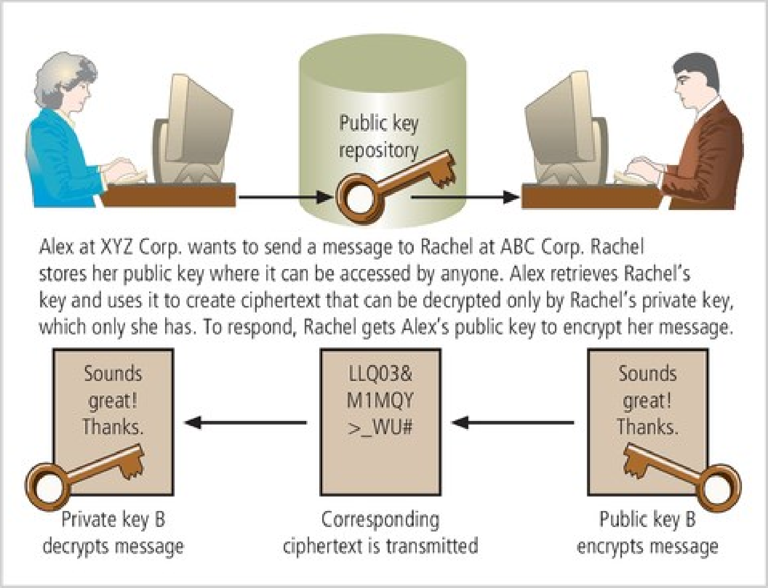

Public key repository
Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves Rachel's key and uses it to create ciphertext that can be decrypted only by Rachel's private key, which only she has. To respond, Rachel gets Alex's public key to encrypt her message.
Sounds great! Thanks.
LLQ03& M1MQY >_WU#
Sounds great! Thanks.
Private key B decrypts message
Corresponding ciphertext is transmitted
Public key B encrypts message

Figure 4. Example of Asymmetric Encryption (Michael, E. W., & Herbert, J.M., 2018)

Methods of encrypting plaintext

Encryption algorithms in use today are well known and kept public knowledge. These Encryption algorithms use either of two methods of encrypting plaintext: the bit stream method or the block cipher method. In the bit stream method, each bit in the plaintext is transformed into a cipher bit one bit at a time to derive the ciphertext. In the block cipher method, the message is divided into blocks, for instance, block sizes of 8-bit, 16-bit, 32-bit, or 64-bit block sizes, and then each block of plaintext bits is transformed into an encrypted block of cipher bits using the encryption algorithm and a key.

Symmetric encryption algorithms

There are some well-known symmetric encryption algorithms or cryptosystems such as the Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES).

DES uses a 64-bit block size and a 56-bit key. However, nowadays, a 56-bit key size does not provide acceptable levels of security. Triple DES (3DES) was created to provide a level of security far beyond that offered in DES. The successor of 3DES is AES. AES implements a block cipher which is called the Rijndael Block Cipher, using a variable block length and a key length of 128, 192, or 256 bits.

Asymmetric encryption algorithm

A well-known asymmetric encryption algorithm or cryptosystem is RSA. The name is derived from Rivest-Shamir-Adleman, the algorithm's developers, and was the first public-key encryption algorithm developed and published for commercial use. RSA is embedded in basically all widely existing Web browsers such as Google Chrome and Microsoft Internet

Explorer to provide security for public-use encryption applications such as e-commerce applications.

These web browsers use HTTPS for secure or encrypted communications over a computer network. HTTPS (Hypertext Transfer Protocol Secure) is an extension of the insecure or unencrypted HTTP (Hypertext Transfer Protocol).

In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, its predecessor, Secure Sockets Layer (SSL). TLS and SSL use the RSA algorithm for encryption.

The future of encryption in IT security

The security of any cryptosystem in practice depends in part on its mathematical design properties. For instance, the mathematical security of modern AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) /Diffie-Hellman cryptosystems rely on the assumption that the computational complexity of the mathematical principles used is too large to be solved in a reasonable time by hackers using currently available computing technology.

As an example, the security of RSA system is closely related to the problem of factoring large composite integers into a product of prime numbers. This is a problem that has been studied in number theory for centuries, yet mathematicians still have not discovered efficient algorithms to solve them. This gives us some confidence about the computational difficulty and its application in cryptography.

However, mathematical improvements and improved computer technology over the last three decades have made such problems solvable in less time than previously assumed. Longer keys are now required to guarantee a given security level against the best-known attack algorithms.

So far today, in general, gradual increases to key lengths have been sufficient to compensate for problem-solving computing technology and mathematical advances. However, it remains a real possibility that future algorithmic research breakthroughs in mathematics and computer technology could make systems such as RSA insecure for any practical key lengths.

Demonstration of encryption (Using Caesar cipher)

Caesar cipher is a very simple encryption method that has been in use for thousands of years (Lambert, 2019). It was used by the military commanders of the Roman emperor Julius Ceaser. This encryption strategy replaces each character in the plaintext with the character that occurs a given distance away in the sequence of a character set, such as the English alphabet character set. For positive distances, the method wraps around to the beginning of the sequence to locate the replacement characters for those characters near its end.

For example, using the English alphabet character set, if the distance value of a Caesar cipher equals three characters, the string "security" would be encrypted as " vhfxulwb". To decrypt this ciphertext back to plaintext, we apply a method that uses the same distance value but looks to the left of each character in the English alphabet character set for its replacement (please see Figure 13. A python Caesar cipher encryption and decryption example results in Appendix B).

Implementation

Caesar cipher would be implemented here using Python programming code. The English alphabet character set is represented in computers using the ASCII (American Standard Code for Information Interchange) codes. Small letters a to z are represented with 97 through 122, while capital letters A to Z are represented with 65 through 90.

In python programming, “ord” function returns the ordinal position of a character value in the ASCII sequence, whereas “chr” function is the inverse function that returns a character. These functions were used to achieve the Caesar cipher encryption.

Two functions were written, one function (encrypt function) for encryption (please see Figure 11. A python encryption function in Appendix B) and one function (decrypt function) for decryption (please see Figure 12. A python decryption function in Appendix B). One word lower case letter was used in the demonstration.

Early History of IT Security

The concept of information security started as computer security, which involved the need to secure the physical location of computer technology from outside threats since the primary threats to security were predominantly physical such as physical theft of equipment, espionage against products of the systems, and sabotage. Computer security was a straightforward process composed predominantly of physical security and simple document classification schemes, however today, the term has evolved into information security, and the scope represents all actions taken to preserve computer systems from losses.

The need for computer security arose during World War II as a national security issue when the first mainframe computers were developed and used to assist in computations for breaking the encrypted messages from enemy cryptographic devices like the German code machine called Enigma.

Mainframe also called "big iron" is a type of computer that is generally known for its large size, amount of storage, processing power and high level of reliability. It is primarily used by government institutions and large organizations for mission-critical applications requiring high volumes of data processing.

The Enigma machine is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication. The Enigma machine was employed extensively by Nazi Germany during World War II, in all branches of the German military.

Figure 5. The Enigma (Michael, E. W., & Herbert, J.M., 2018)

During these early years, information security was all about physical security on the military sites where these mainframe computers were located, and access to sensitive military locations was controlled through physical controls such as badges, keys, and the facial recognition of authorized personnel by security guards.

One of the first known security problems that fell outside of physical security occurred in the early 1960s when a systems administrator was working on a MOTD (message of the day) file while another administrator was editing the password file. A software malfunction mixed the two files, and the entire password file was printed on every output file. Such a security breach as this suggested that physical security alone was no longer enough for the protection of these systems.

During the Cold War (geopolitical tension between the Soviet Union and the United States and their respective allies) after World War II, many more mainframe computers were employed to accomplish more complex and sophisticated tasks. These mainframes communicated by mailing magnetic tapes between computer centers. This process of communication was considered cumbersome, and for this reason, in 1968, the Department of Defense's Advanced Research Projects Agency (ARPA) developed the ARPANET project (developed by Dr. Larry Roberts). ARPANET was a redundant, networked communications system between the mainframes in computer centers to support the military's exchange of information. ARPANET evolved into what we now know as the Internet, and Dr. Larry Roberts became known as its founder.

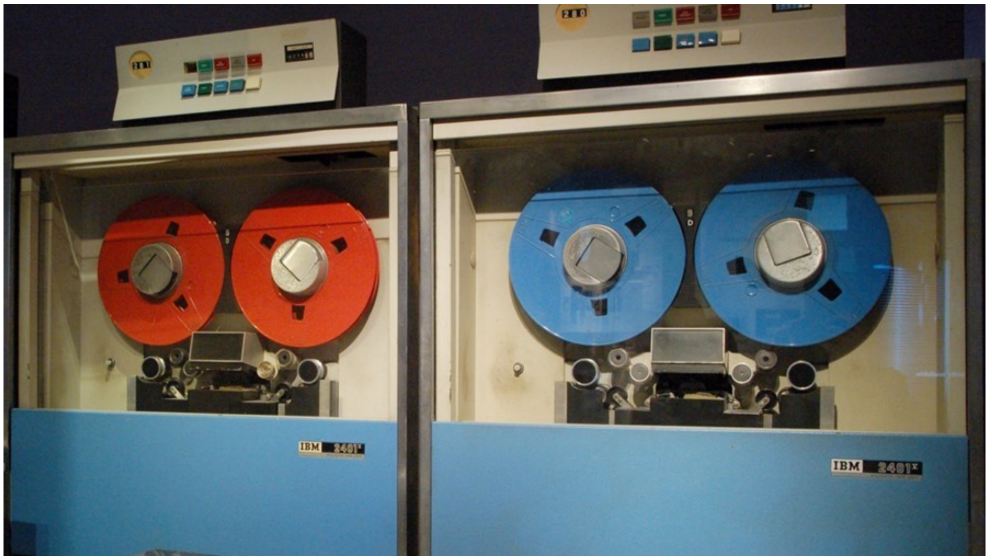


Figure 6. IBM 2401 mainframe and Magnetic tapes (Ian, S., 2017)

In the 1970s ARPANET became more popular, having more number of hosts and users on ARPANET. This explosion in the numbers of hosts and users on ARPANET increased the potential for its misuse.

High frequency of computer security violations started coming up due to the following fundamental problems with ARPANET security;

- Individual remote sites did not have sufficient controls and safeguards to protect data from unauthorized remote users.
- The vulnerability of password structure and formats
- Lack of safety procedures for dial-up connections; Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET
- Nonexistent user identification and authorizations

In February 1970, the RAND Corporation published a paper called RAND Report R-609 for the Department of Defense. This paper went beyond protecting the physical location of computing devices and was the first widely recognized published document to identify the role of management and policy issues in computer security.

The scope of computer security expanded significantly from the safety of physical locations and hardware to include:

- Data security, limiting random and unauthorized access to that data
- The Involvement of personnel from multiple levels of the organization in information security

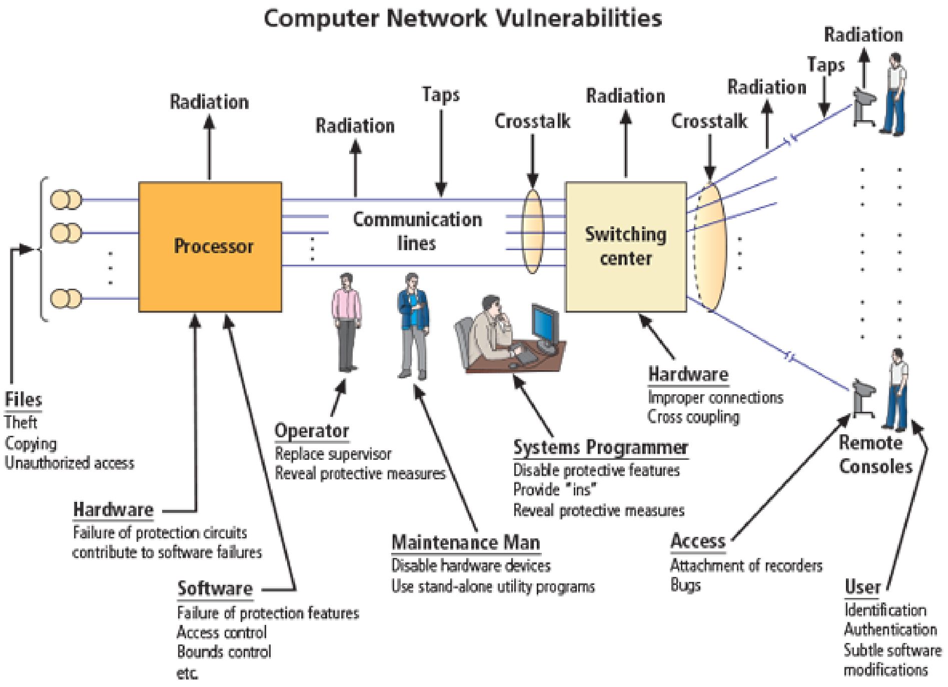


Figure 7. Illustration of Computer Network Vulnerabilities from RAND Report R-609 (Michael, E. W., & Herbert, J.M., 2018)

The first computer virus, called “Creeper system”, was an experimental self-replicating virus released in 1971. Victim’s screen displayed the phrase: “I’m the creeper, catch me if you can.” Creeper was a worm, a type of computer virus that replicates itself and spreads to other systems; It was filling up the hard drive until a computer could not operate any further. This virus was created by BBN (Bold, Beranek and Newman) technologies in the US.

In the late 1970s, the microprocessor brought the personal computer (PC) and a new age of computing. The PC became the workhorse of modern computing, moving it out of the data center. This meant more number of hosts and users on ARPANET.

This decentralization of data processing systems in the 1980s gave rise to networking; the interconnecting of PCs and mainframe computers, which enabled the entire computing community to make all its resources work together. This is called the internet.

The core technologies of the Internet TCP and IP were finalized in 1981. There was no mention of security in these technologies, indicating that at that time the technology world was not concerned about information security (Manish, A., Alex, C., & Eric, P., 2014).

The internet created a fertile environment for information security compromises to flourish such as the 1988 Morris worm considered the first Internet worm. It is estimated to have brought down 10% of the internet, the largest fraction of the Internet ever to be brought down.

Morris worm led the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense to create the Computer Emergency Response Team (CERT) in 1988 to address network security due to rising security breaches.

IT security in the last 30 years

This rise to the Internet, the first global network of networks towards the close of the 20th century, came as a result of networks of computers becoming more common, as did the need to connect them to each other.

The Internet was made available to the general public in the 1990s after decades of being the domain of government, academia, and dedicated industry professionals. The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet connected local area network (LAN). After the Internet was commercialized, the technology became pervasive, reaching almost every corner of the globe with an expanding array of uses.

Microsoft released Windows 95 operating system in 1995. Windows 95 was designed primarily as a stand-alone single-user desktop operating system and therefore had almost no security precautions. However, Windows 95 supported TCP/IP internet protocol, thereby bringing TCP/IP into mainstream businesses.

As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats.

In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations. Antivirus products became extremely popular, and information security began to emerge as an independent discipline.

Today, the Internet brings millions of unsecured computer networks and billions of computer systems and devices into continuous communication with each other.

Recent years have seen a growing awareness of the need to improve information security, as well as a realization that information security is important to national defense. The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure.

Another growing concern is the threat of nation-states engaging in information warfare, and the possibility that business and personal information systems could become victims if they are undefended.

Historically, the United States has been a leader in the development and implementation of information security legislation to prevent misuse and exploitation of information and information technology. In its global leadership capacity, the United States has demonstrated a clear understanding of the importance of securing information and has specified penalties for people and organizations that breach U.S. civil statutes.

Since 2000, Sarbanes-Oxley (SOX) and other laws related to privacy and corporate responsibility have affected computer security.

The Sarbanes-Oxley Act of 2002, also known as SOX or the Corporate and Auditing Accountability and Responsibility Act, seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.

The attack on the World Trade Centers on September 11, 2001 resulted in major legislation changes related to computer security, specifically to facilitate law enforcement's ability to collect information about terrorism. For example, The USA PATRIOT Act of 2001, which provides law enforcement agencies with broader autonomy to combat terrorism-related activities, while providing them with Appropriate Tools Required to Intercept and Obstruct Terrorism.

Among other laws are The U.S. Copyright Law and The Freedom of Information Act (FOIA). The U.S. Copyright Law is for published works, including electronic formats. Fair use allows copyrighted materials to be used to support news reporting, teaching, scholarship, and similar activities, as long as the use is for educational or library purposes, is not for profit, and is not excessive, The Freedom of Information Act (FOIA) allows any person to request access to federal agency records or information not determined to be a matter of national security.

There are also international laws helping to foster IT security such as the Council of Europe Convention on Cybercrime, which created an international task force to oversee a range of security functions associated with Internet activities and standardized technology laws across international borders.

The Digital Millennium Copyright Act (DMCA). This is the American contribution to an international effort by the World Intellectual Properties Organization (WIPO) to reduce the impact of copyright, trademark, and privacy infringement.

However, due to political complexities of relationships among nations and differences in culture, few current international laws cover privacy and information security and most times are limited in their enforceability across countries.

Problem Statement

One surprisingly prevalent issue that companies face when it comes to information security is their lack of a formal corporate security program or plan and the inefficiency of these plans when available. this proactive approach to information security is the missing ingredient with many businesses. The absence or inefficiency of a security program or plan in an organization leads to failure to have a cutting-edge comprehensive Information Security plan, failure to adopt a response plan prior to a breach, failure to view data security as a "business problem" and not just an "IT problem, failure to understand the true threat against their employees, suppliers and ultimately their data thereby exposing the organization to greater risk of an attack or data breach.

Many organizations lack the modern tools or the expert configurations necessary to meet the challenges of today's dynamic threat landscape. Organizations of all shapes and sizes face a diverse and ever-changing security threat landscape. From targeted phishing attacks to sophisticated malware, many businesses lack the modern tools to meet this growing challenge and even when these tools available, they may not be configured properly. Some organizations still run perimeter-only security solutions or signature-based antivirus which might prove ineffective in mitigating new forms of threats, while others have purchased but not effectively implemented newer tools like EDR (Endpoint Detection and Response) for threat detection and response.

Prevalent absence or inefficient security education, training, and awareness program in organizations. Often times, businesses concentrate on securing the network perimeter with firewalls, deploying advanced anti-malware solutions, and implementing other technological controls such as spam filters and endpoint protection systems, yet they fail to provide effective security awareness training for employees. Even when security awareness training programs are developed, they are often once-a-year classroom-based training sessions that are forgotten quickly. One-quarter of all data breaches in 2018 were caused by human error (Tara, 2019).

Most organizations neglect physical security over information (logical) security. Organizations tend to focus their security efforts on traditional data breaches ranging from low-level script kiddie attacks to complex and sophisticated cyberattacks perpetrated by organized crime groups without taking the time to establish the link these measures have with physical security such as physical access control. A state of the art security measures could be put in place, but if an adversary can easily wander into ta restricted area such as the server room or data center due to a lack of proper physical access control, most of the carefully designed logical security measures may be rendered useless.

Some organizations choose not to comply with information security laws pertaining to their business for many reasons, including financial ones. An organization may feel that information security laws do not directly affect them and thus choose not to adhere to them or take them seriously however, they are mistaken. Federal and state laws require organizations to comply with information security laws, and failure to do so often results in significant penalties or fines. In some situations, organizations may also be susceptible to lawsuits.

Discussion

Despite all efforts to protect IT systems, they remain vulnerable in some way, and we continue to get hacked. Even high technology companies that literally invest millions of dollars annually in security measures end up being attacked successfully. Below is a discussion on some prominent data breaches over the years that will help us to analyze information security standing in this day and age.

On Nov 21, 2017, Uber Technologies, Inc., an American company popularly known for its ridesharing services announced that two hackers were able to get the names, email addresses, and mobile phone numbers of 57 million users of the Uber app., and the driver license numbers of 600,000 Uber drivers. The hackers were able to gain access to Uber's GitHub account, where they found the username and password credentials to Uber's AWS (Amazon Web Services) account which gave them full access to Uber's information on AWS. Uber paid the hackers $100,000 to destroy the data with no way to verify that the data was destroyed. Uber had to fire its CSO (Chief Security Officer) because of the breach, as the blame was placed on him. The breach cost Uber dearly in terms of reputation and money (Uber's valuation dropped from $68 billion to $48 billion within the next month after the announcement).

On December 19, 2013, Target Corporation, the 8th-largest retailer company in the United States announced an unauthorized access to its payment card data that impacted certain customers making credit and debit card purchases in its U.S. stores. The retail giant declared that that hackers had gained access to its point-of-sale (POS) payment card readers, and had collected about 40 million credit and debit card numbers. Also, personally identifiable information (PII) of about 110 million of its customers was compromised. That included full names, addresses, email addresses, and telephone numbers. The company estimated the cost of the breach at $162 million including legal fees. Following this incident, Target’s CIO (Chief Information Officer) resigned in March 2014, and its CEO (Chief Executive Officer) resigned in May 2014.

Target made a mistake that led to this attack by giving remote access to its network to its HVAC (Heating, ventilation, and air conditioning) vendor Fazio Mechanical Services. This company was then targeted with a social engineering phishing email that installed malware onto their system. The hacker then used this to route into Target’s network, installing a malware that recorded and extracted the information for every credit and debit card used on an infected POS machine.

On October 3, 2017, Yahoo, the once dominant Internet giant, an American web services provider headquartered in Sunnyvale, California, and now owned by Verizon Media announced it had been the victim of the biggest data breach in history likely by “a state-sponsored actor”. All of its three (3) billion user accounts were compromised. The attack compromised the real names, email addresses, dates of birth, telephone numbers, security questions, and answers of three billion users. The breaches knocked an estimated $350 million off Yahoo’s sale price.

On January 19, 2009, Heartland Payment Systems, Inc., then the sixth-largest payments processor in the U.S., now acquired by Global Payments Inc., announced that its processing systems were breached in 2008, 134 million credit and debit cards were exposed through SQL (Structured Query Language) injection that installed spyware on Heartland's data systems. The company was deemed out of compliance with the Payment Card Industry Data Security Standard (PCI DSS) and was not allowed to process the payments of major credit card providers until May 2009. The company also paid out an estimated $145 million in compensation for fraudulent payments.

On October 7, 2014, JPMorgan Chase & Co., an American multinational investment bank and financial services holding company headquartered in New York City disclosed that it was the victim of a hack during the summer of 2014 that compromised users' contact information; name, address, phone number and email address and internal JPMorgan Chase information relating to such users have been compromised. The compromised data impacted approximately 76 million households and 7 million small businesses.

JPMorgan Chase & Co. was reportedly spending $250 million on security every year at the time of this breach (Taylor, 2018). Yet, the hackers were able to gain "root" privileges (the highest level of administrative privilege) on more than 90 of the bank's servers. Which meant they could take such actions as transferring funds and closing accounts.

The above examples are just few of the numerous attacks that have become prevalent in the field of Information technology today.

Summary of findings

Table 1

Summary of findings from the discussion

S/N	Company	Year announced	Impact	Damage	Reason
1	Uber Technologies, Inc.	2017	57 million Uber users and 600,000 drivers	$68 billion to $48 billion drop in Uber's valuation, $100,000 paid to hackers	Password and username not securely stored
2	Target Corporation	2013		$162 million	Social Engineering – Phishing Email
3	Yahoo	2014	3 billion user accounts	$350 million off Yahoo's sale price	Likely by a State sponsored hacker
4	Heartland Payment Systems, Inc.	2009	134 million credit cards	$145 million in compensation for fraudulent payments	Spyware in data systems
5	JPMorgan Chase & Co.	2014	76 million households and 7 million small businesses	Loss in reputation, undisclosed monetary value	Root access to servers by hackers

From the summary of findings, we can see the effect of security breaches at a glance. Breaches cost money and reputation, which might lead to the complete closure of an organization.

Breaches could be as a result of a state-sponsored actor by governments looking to collect information or spy on their citizens.

The findings also prove that we cannot assume that any system is safe, being hacked is inevitable. For instance, although JPMorgan Chase & Co. was spending $250 million on security every year at the time, hackers were still able to get hold of the systems.

Conclusion

IT security was not always an issue and did not occur to the first developers and users of computer networks. However, with the advent of the internet and the proliferation of devices in constant communication over computer networks and the internet, IT security can no longer be ignored

IT security is referred to as the prevention of unauthorized access to organizational information assets to maintain confidentiality, integrity, and availability.

The cryptographic technique of encryption is the bedrock of modern information security. Encryption involves converting plain text into forms unintelligible to unauthorized parties using encryption algorithms and keys. Encryption algorithms can be symmetric (requires the same private key for encryption and decryption - for symmetric encryption) or asymmetric (requiring two different keys private and public keys for encryption and decryption – for asymmetric encryption).

Information security started as computer security (involved only physical security), which was needed during World War II to protect military sites containing mainframe computers used in computations such as in breaking enemy cryptographic codes like the German Enigma machine code.

After world war II, During the Cold War, many more mainframes were employed to perform complex tasks. These mainframes communicated by mailing magnetic disks between computer centers. This cumbersome form of communication led to ARPANET, a network of computer centers for the exchange of information.

ARPANET became more popular in the 1970s, with more hosts being connected. This increased the potential for misuse, coupled with the fact that individual remote sites had insufficient controls and safeguards to protect data from unauthorized remote users. This led RAND Corporation to publish the RAND Report R-609 for the Department of Defense, which included data security and the involvement of personnel from various levels of organization in the information security function, thus moving information security beyond just physical security.

In the late 1970s, the microprocessor brought the personal computer (PC). The networking of PCs and the mainframe computers on the ARPANET gave rise to the internet. The core Internet protocols TCP and IP completed in 1981 had no security and gave rise to security breaches, including the 1988 Morris worm that led the Defense Advanced Research Projects Agency (DARPA) within the Department of Defense to create the Computer Emergency Response Team (CERT) in 1988 to address network security.

The Internet was made available to the general public and commercialized in the 1990s. Microsoft released Windows 95 operating system in 1995. It had almost no security precautions. It was GUI (Graphical User Interface) based and a stand-alone single-user desktop operating system, which made it very successful in the market. Windows 95 supported TCP/IP internet protocol, thereby bringing TCP/IP into mainstream businesses.

As networked computers became the dominant style of computing, information became more exposed to security threats. In the late 1990s and into the 2000s, many large corporations began integrating security into their organizations. Antivirus products became extremely popular, and information security began to emerge as an independent discipline.

Today, the internet connects billions of devices, and there is increasing awareness even among governments on the importance of information security.

The United States has been a leader in the development and implementation of information security legislation to prevent misuse and exploitation of information and information technology such as The Sarbanes-Oxley Act of 2002, The USA PATRIOT Act of 2001, The U.S. Copyright Law and The Freedom of Information Act (FOIA).

There are also international laws helping to foster IT security, such as the Council of Europe Convention on Cybercrime and The Digital Millennium Copyright Act (DMCA).

Despite these efforts towards IT security, there are certain problems facing information security today. Among these problems are lack of a formal corporate security program or plan and the inefficiency of these plans when available in organizations, lack of the modern tools or configurations necessary to meet the challenges of today's dynamic threat landscape, Prevalent absence or inefficient security education, training, and awareness program in organizations, most organizations neglect physical security over information (logical) security, and non-compliance with information security laws.

Some prominent data breaches that have occurred over the years are Uber Technologies, Inc. (affected 57 million users and 600,000 Uber drivers), Target Corporation (affected about 40 million credit and debit card numbers and about 110 million customers), Yahoo (affected three (3) billion user accounts), Heartland Payment Systems, Inc. (affected 134 million credit and debit cards), JPMorgan Chase & Co. (affected approximately 76 million households and 7 million small businesses.).

These breaches not only came with reputational damage for the organizations but also monetary losses and legal issues in some cases.

Recommendations

In order to provide meaningful protection for information assets in today's dynamic information security landscape, a proactive approach or strategy must be adopted to stay alert at all times. From the problems and conclusions, the following recommendations are provided.

Information Security Planning

Every security effort within an organization should start with Information Security Planning. This plan involves developing a Policy, Information Security Planning, and Risk management plan.

A security policy involves a deliberate course or principle of action adopted or proposed to guide decisions on achieving the overall security needs and IT security needs of the organization. Security policy acts as the foundation or blueprint for Information Security Planning.

Information Security Planning is based on the security policy to guide organizational security efforts and focus resources towards achieving its security objectives. It involves plans on the systems such as hardware and software controls to be put in place to achieve organizational security objectives.

There should also be a plan for risk management. A risk management plan offers the best way to ensure that the risk of data breaches is minimal such as through regular security training of staff on the need for acceptable security practices. It would help in business continuity, Security monitoring & disaster recovery in the off chance that disaster strikes. This involves risk identification, risk assessment, and risk control.

Risk identification would help specify the possible risks and threats facing the organization.

A risk assessment would help ascertain the possible impact of these risks to the organization should they occur. It proceeds by selecting identified risk scenarios that are relevant to an organization and analyzing their impacts in the event that they materialize.

Risk control would help to plan for ways to mitigate these risks or reduce them to an acceptable level and what to do if they occur. It involves contingency planning strategies such as a disaster recovery plan available to an organization for responding to adverse events. Disaster recovery typically focuses on restoring systems and operations at the original site where the disaster occurred.

Information Security Blueprint

An information security blueprint is a detailed implementation of an information security framework (also known as an information security model). Organizations should adopt a recognized or widely accepted information security model backed or promoted by an established security organization or agency. Some prominent frameworks are: The ISO 27000 Series, NIST Security Models.

These security frameworks help in the design and implementation of security infrastructure in an organization. It acts as a starting point for the development of organization-specific security guidance. It also offers guidelines and directions for implementing standard information security management.

A security framework is meant to provide a high level, general description of the important security areas in the process of initiating, implementing, or maintaining information security in an organization.

It provides information on how to implement security infrastructure and set up an information security management system. It can also provide a means of assessing and building an information security program to ensure that it is of standard.

Modern Security Tools

Although there is no product portfolio that will be right for every organization, there are several IT security and Cybersecurity tools that are basic, yet highly effective. Tools such as antivirus and firewalls, IDPSs (Intrusion Detection and Prevention Systems), and honeypot (also called lures, decoys, or flytraps) and honeynet (Several honeypot systems connected together on a network segment), could prove very useful in protecting information systems within the organization.

While first line of defense security tools, such as firewalls and anti-virus software, can be effective at identifying and potentially stopping known forms of malware and viruses attacking companies every day, they are blind to signature-less and zero-day malicious Risk scenarios (cyber-attack targeting a software vulnerability which is unknown to the software vendor or to antivirus vendors) used by black hat hackers today. Therefore, approaches such as vulnerability scanning (The attempted sanitization of code environments through periodic penetration testing and code review, typically performed after updates are made to an application), deploying software patches (Code developed to apply fixes to software and systems after an issue has been identified) as soon as possible, and installing new software versions as soon as they are released, would help to detect software vulnerabilities as soon as possible for mitigation.

Configurations, changes, and modifications to these tools should be handled with proper configuration management (CM) since Information systems are typically in a constant state of evolution with upgrades to hardware, software, and firmware and even possible modifications to the system's surrounding environment. CM would help to evaluate proposed changes, track changes through completion, maintain systems inventory, and documentation of which components have been modified and why which streamlines the audit process.

Data Security

Data Security involves securing data and information, both stored and in transit. Encryption technology remains one of the most prominent ways to secure data and an important Cybersecurity tool. VPN (Virtual Private Network) is employed to secure remote connections over the internet, or through service providers used by telecommuters, vendors, and branch communication.

Encryption Technology

Data being communicated in the day to day operations of a business should be encrypted to avoid disclosure even when the data is intercepted. Encryption should also be applied to organizational procedures, technical work instructions, internal processes, and policy documentation for protection against theft of trade secrets.

VPN (Virtual Private Network)

Installation of a virtual private network (VPN) provides protection for remote access data in transmission through telecommuters, between branch offices, and even vendors. VPN also uses encryption technology and provides a secure way for remote communication.

Security Education, Training, and Awareness

The human component of information security remains its weakest link especially due to the high susceptibility of humans to social engineering schemes like phishing attacks. Therefore, there is the ever-present need to prepare people (both users and administrators) for the current and future IT security needs through security education, training, and awareness.

In order to expect good information security, the humans who develop, use, and operate information systems ought to be well prepared with the right knowledge they need in their day to day interactions with the systems.

There should be a security program implemented to provide security education, training, and awareness to all staff on induction and regularly communicate security updates. Security programs within an organization should cover all the major threats faced by an organization, including web-based attacks, malware, and social engineering scams via telephone, text message, or social media channels and phishing emails. Security conferences could also be incorporated as an approach towards a good security program. This approach is required to keep the organization’s information security assets safe.

Security Awareness

The people involved with information technologies should be properly informed or made aware of the need to protect system resources against breaches. This could be done through an information Technology security awareness program.

Security Education

This involves preparing people through formal education or certificate. This would help to prepare people properly with the right information about IT security needs.

Security Training

This involves providing those involved with information technology with detailed information on IT security and hands-on training to perform their tasks securely.

Security Conferences

Incorporating security conferences in security programs within an organization could also serve as an avenue for security awareness and training. Such conferences are;

The DEF CON Conference. The DEF CON Conference was first held on June 9, 1993. DEF CON is one of the world's most popular cybersecurity technical conferences. Started in June of 1993 by Jeff Moss, it opened in Las Vegas with roughly 100 people. Today the conference is attended by over 20,000 cybersecurity professionals from around the world.

The RSA Conference. The RSA (Rivest, Shamir, and Adleman) Conference is a series of IT (Information Technology) security conferences. Approximately 45,000 people attend one of the conferences each year. RSA Conference was founded in 1991 as a small cryptography conference. RSA conferences take place in the United States, Europe, Asia, and the United Arab Emirates each year.

Physical Security

Physical security deals with the Physical Security Control methods of protecting an organization's physical presence. Physical security measures have to be considered carefully to restrict access to unauthorized individuals in areas they should not be within the organization's facilities since physical access to information assets could render all logical protections useless. Physical security controls that could be considered are;

Walls, Fencing, and Gates

Walls, Fencing, and Gates are used to restrict unauthorized access to physical locations the organization owns or controls. Concrete wall barriers are provided close to car parks to withstand the possible blast of a car bomb from damaging the organization's building and assets inside.

Guards

Human guards are employed to make the responsive evaluation of each situation as it arises and make reasoned responses such as opening up the gates for authorized individuals, especially when the gates are static barriers.

Guard dogs are also used. They can detect intrusions that human guards cannot, because of their keen sense of smell and hearing. Guard dogs are more suitable in situations that would risk the life of a human guard.

ID Cards and Badges

They serve as simple forms of biometrics and allow an organization to restrict access to sensitive areas within the facility. An identification (ID) card is typically coded and carried concealed, whereas a badge is worn and visible, having the wearer's name or photograph or even both.

Tailgating (when an authorized person opens a door, and other people also enter) is an inherent problem to this method of physical access control, which should be considered carefully. Tailgating becomes especially dangerous when the tailgater is not authorized to enter or access the area in question. One way to combat this problem is by making employees aware of tailgating through a security awareness program.

Locks and Keys

There are Mechanical, electromechanical, and biometric forms. The mechanical lock may rely on a metallic key that releases secured loops of steel, aluminum, or brass. The mechanical lock may also rely on a dial that aligns to a combination of numbers and then retracts a securing bolt. Electromechanical locks may use inputs from magnetic strips on ID cards, radio signals from badges, or personal identification numbers (PINs) as key to unlock them. Biometric locks are the most sophisticated locks, they may use Finger, palm, and hand readers, iris and retina scanners, voice or signature readers as key to unlock them.

Locks and Keys help to restrict unauthorized access to secured locations.

Fire Detection and Response

The most damage to property, personal injury, and death in organizations is caused by fire.

Manual and Automatic Fire Detection are required. When manual detection is used, people should be designated as floor monitors against false alarms.

Fire suppression systems such as Portable extinguishers and Gaseous (or chemical gas) emission systems should also be installed.

Mantraps

This is an enhancement to lock and keys. A person wishing to gain access to an area of the facility enters the mantrap, requests access through some form of electronic or biometric lock and key and then is given access into the facility or area he or she wishes to access.

If access is denied, the person cannot leave the mantrap until a security official decides on whether to allow the person in or let the person out.

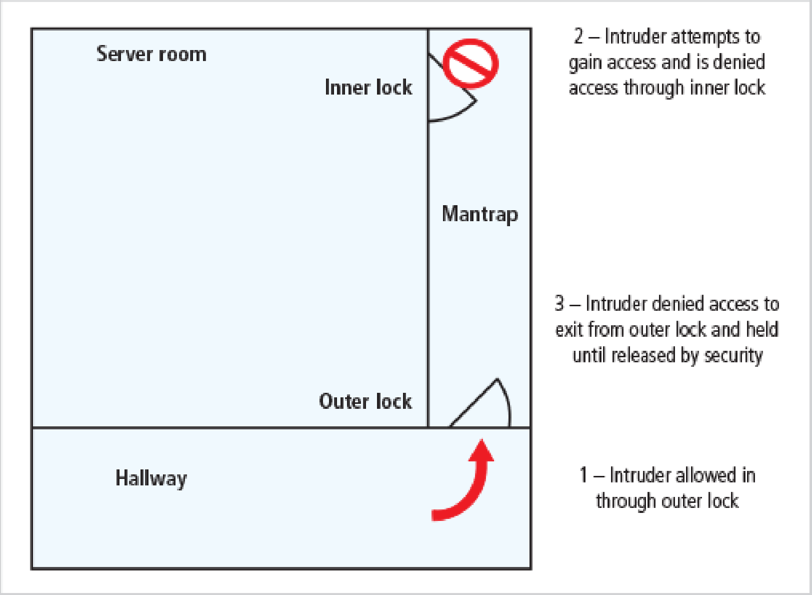

Server room
Inner lock
Mantrap
Outer lock
Hallway
2 – Intruder attempts to gain access and is denied access through inner lock
3 – Intruder denied access to exit from outer lock and held until released by security
1 – Intruder allowed in through outer lock

Figure 8. Mantraps (Michael, E. W., & Herbert, J.M., 2018)

Electronic Monitoring

This involves video monitoring cameras attached to Video Cassette Recorders (VCRs) or similar machinery that capture the video feed, the feed is then monitored through a system such as Closed-Circuit Television (CCT) systems.

One major advantage of Electronic Monitoring equipment is that they can record events that human guards and guard dogs might miss.

Alarms and Alarm Systems

They are used to notify people or systems when a predetermined event or activity occurs such as a fire, a break-in, flooding, a loss of power. They rely on different types of sensors, such as thermal detectors, glass breakage detectors, motion detectors, contact sensors, and weight sensors.

Interior Walls

Computer rooms, electrical wiring closets, and other high-security areas within the warehouse should be surrounded by firewall-grade walls (walls that limit the spread of fire damage should a fire break out in an office or an area of the warehouse) to provide for both physical security against potential intruders (such as burglars) and fires.

Heating, Ventilation, and Air Conditioning

Temperature and Filtration equipment should be put in place to protect against the damages to systems and discomfort to humans from extreme temperatures and particulate contamination.

Humidity and Static Electricity control equipment should also be in place. High humidity levels create condensation problems, and low humidity levels can increase the amount of static electricity in the environment. This might affect information assets.

Villains may enter an unauthorized area of an organization’s facility through ventilation shafts. Ventilation shafts can be completely eliminated if possible since they are a security vulnerability. If they are used, the security team can install wire mesh grids at various points to compartmentalize the runs especially if the ducts are much larger. This would prevent villains from entering the facility through them.

Power Management and Conditioning

This involves Grounding and Amperage. Grounding ensures that the returning flow of current is properly discharged to the ground while Amperage measures ensure that sufficient amperage is supplied to support needed operations in the electrical equipment.

Uninterruptible Power Supply, which is a device that assures the delivery of electric power without interruption in the electrical equipment, is also required.

Emergency Shutoff measure provides the ability to stop power immediately if the current represents a safety risk to people or machines in the organization.

Information Security Laws

Information Security Law is the body of legal rules, codes, and standards that require you to protect that information and the information systems that process it, from unauthorized access. The development of such relevant laws should be encouraged, especially global scale security laws.

Organizations are usually subject to several different information security laws or standards, and they should be strictly adhered to in order to avoid legal consequences and provide better security for information assets. Some standards that an organization may be subject to are:

GDPR (General Data Protection Regulation).

A European Union's standard that guarantees the rights of information owner which an organization may be collecting. Such as the right to deny the collection of personal data and the right to be forgotten upon request by the information owner.

PCI DSS (Payment Card Industry Data Security Standard).

PCI DSS is a security standard for any business handling payment card information such as credit cards, debit cards, ATM cards, store-value cards, gift cards, or other related items. It was designed to enhance the security of customers' account data.

HIPAA (Health Insurance Portability and Accountability Act).

This law deals with the protection of patient information for insurance companies and healthcare providers.

GLBA (Gramm Leach Bliley Act).

This standard deals with information security for financial institutions such as banks and insurance companies. It ensures the safety of clients' private data.

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002, also known as SOX or the Corporate and Auditing Accountability and Responsibility Act, is an important piece of legislation that affects the executive management of publicly traded corporations and public accounting firms. The law seeks to improve the reliability and accuracy of financial reporting, as well as increase the accountability of corporate governance, in publicly traded companies.

Further work

This research project was aimed at helping us see how far we have come in the field of IT security over the years, mistakes made, lessons learned, and how best to tackle the challenges IT security faces today in an exhaustive manner.

However, there is always room for improvement, and further research could be carried out on this topic of the evolution of IT security in the last thirty (30) years – since the time of mainframe. Such topics as “The Strategies to Mitigate Zero-Day Attacks”, and “The Role of AI (Artificial Intelligence) in IT Security” would be good fits as further works on this topic.

References

Gemalto a Thales Company. (2017). First Half 2017 Breach Level Index Report: Identity Theft and Poor Internal Security Practices Take a Toll. Retrieved from https://www.gemalto.com/press/pages/first-half-2017-breach-level-index-report-identity-theft-and-poor-internal-security-practices-take-a-toll.aspx

Ian, S. (2017). No end in sight for magnetic tape storage as IBM and Sony squeeze 201 gigabits per square inch. [web log post]. Retrieved from https://www.telecomtv.com/content/ibm/no-end-in-sight-for-magnetic-tape-storage-as-ibm-and-sony-squeeze-201-gigabits-per-square-inch-15863/

Karl, D.L., & Jan, B. (2007). The History of Information Security: A Comprehensive Handbook. Boston: Elsevier.

Kenneth, K. (2019, JUL 30). 5 of the biggest data breaches ever. Retrieved from https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html

Lambert, K. A. (2019). Fundamentals of Python: First Programs. Boston, Massachusetts: Cengage Learning.

Manish, A., Alex, C., Eric, P. (2014). *Information security and IT risk management.* Hoboken, N.J: John Wiley and Sons, Inc.

Margaret, R. (2018). Cryptography. [web log post] Retrieved from https://searchsecurity.techtarget.com/definition/cryptography

Michael, E. W., & Herbert, J.M. (2018). Principles of Information Security. Boston, Massachusetts: Cengage Learning.

Mike, L. (2015, Nov 25). A History of Information Security from Past to Present. [web log post]. Retrieved from https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present

Morgan, H. (2019, Jan 17). Understanding the ever-changing threat landscape. [web log post]. Retrieved from https://securitytoday.com/Articles/2019/01/17/Tackling-the-Challenges.aspx?Page=1

Robert, J. (2019). 60 Percent of Small Companies Close Within 6 Months of Being Hacked. [web log post]. Retrieved from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Seymour, B. & Kabay, M.E. (2012). Computer Security Handbook. New York, NY: John Wiley & Sons, Inc.

Tara, S. (2019, July 24). ThreatList: Human Error is Behind One Quarter of Data Breaches. [web log post]. Retrieved from https://threatpost.com/quarter-of-breaches-human-error/146662/

Taylor, A. (2018). The 18 biggest data breaches of the 21st century. [web log post]. Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Tim, M. (2019). A Brief History of Cybersecurity [web log post] Retrieved from https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/

Appendix A

Data charts

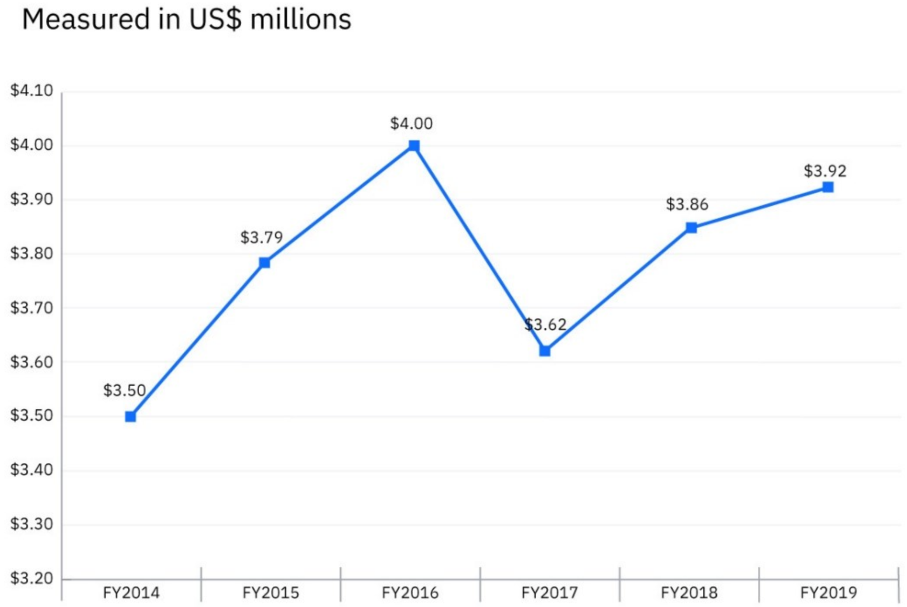


Figure 9. Global Average Total Cost of a Data Breach (IBM, 2019)

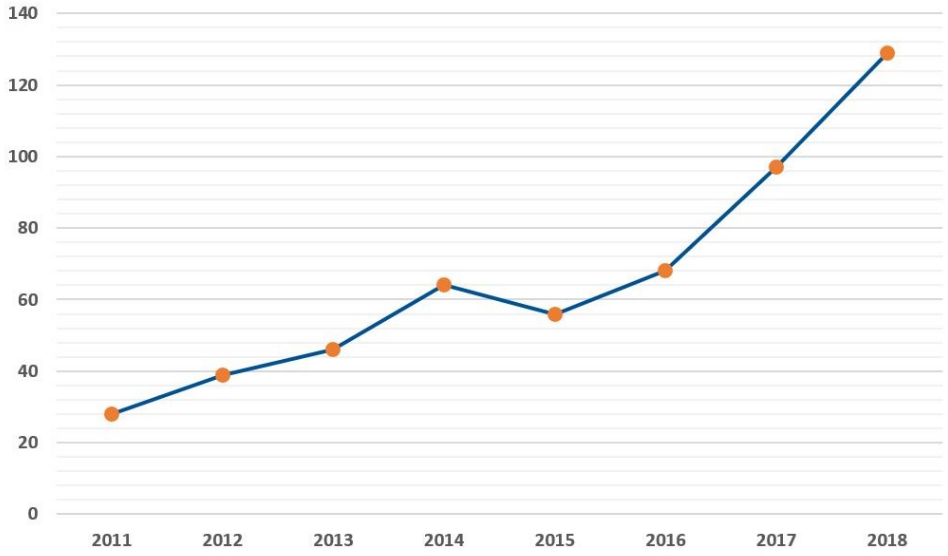
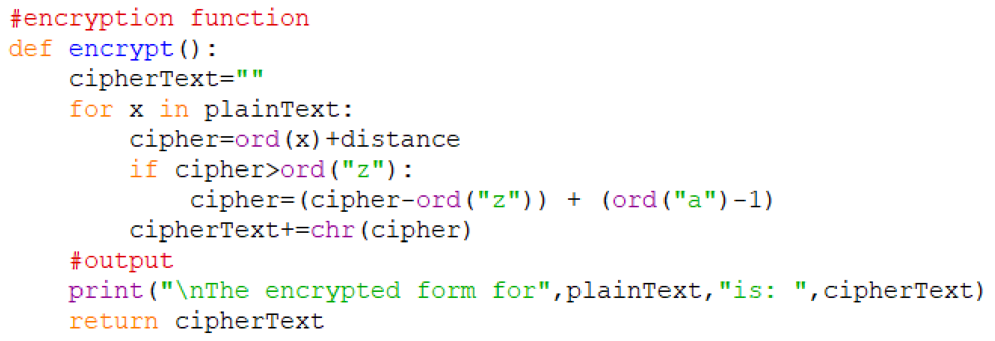


Figure 10. Number of Cybersecurity Breaches Disclosed per Year (Audit Analytics, 2019)

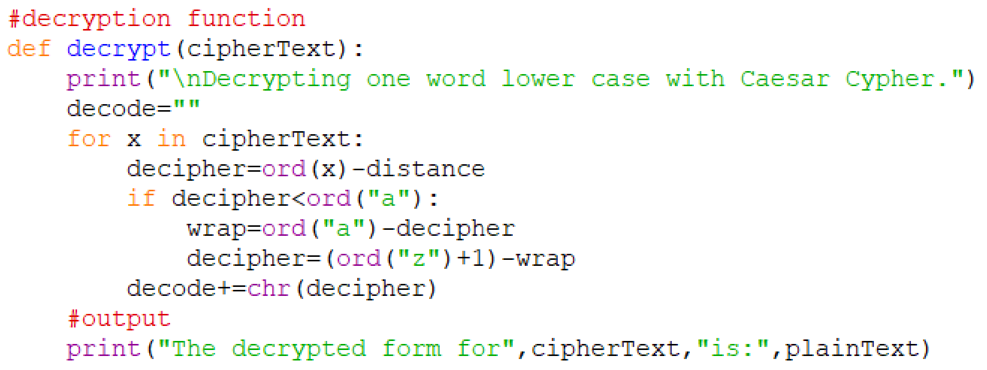
Appendix B

Program Codes and Result



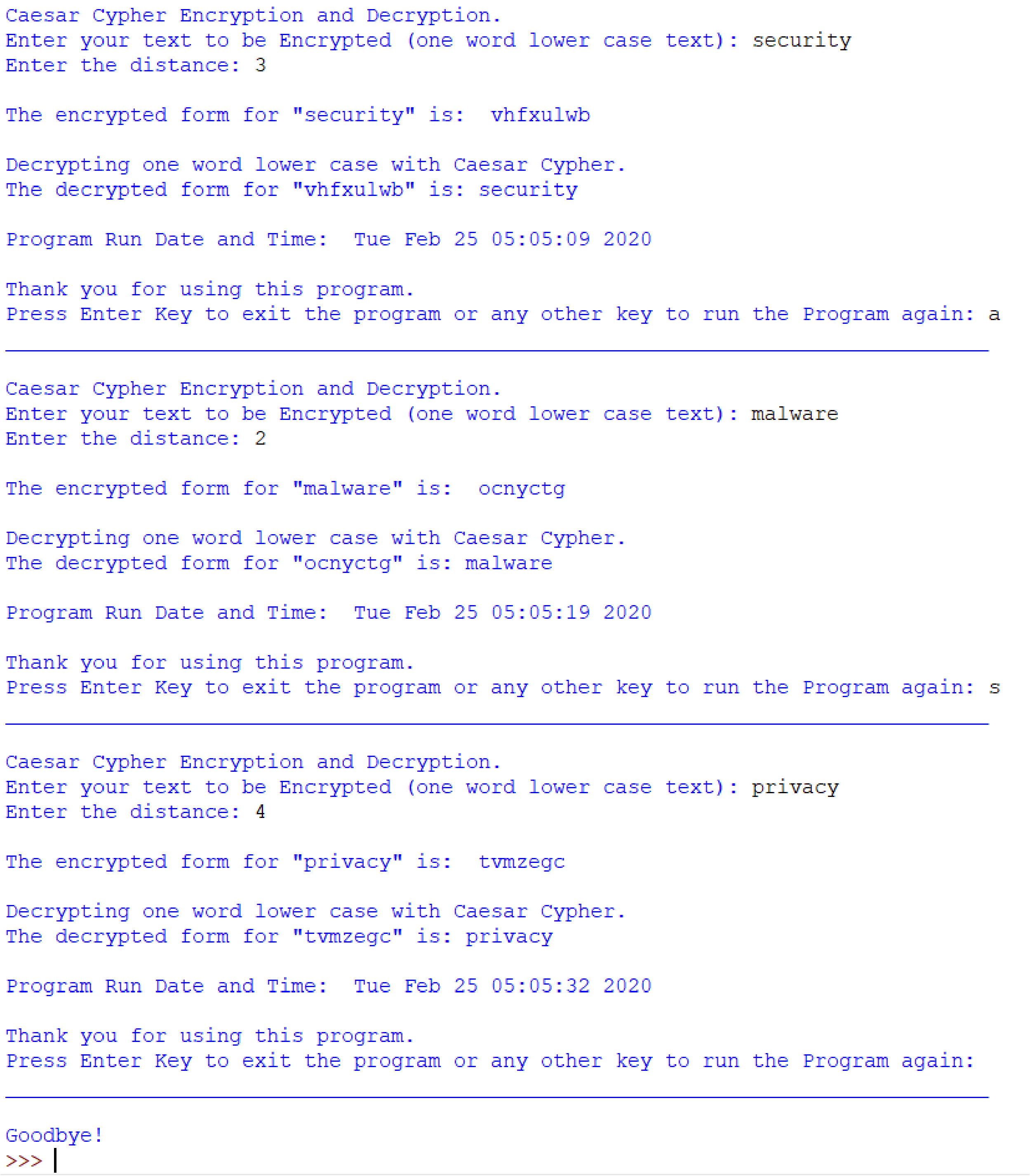
```
#encryption function
def encrypt():
    cipherText=""
    for x in plainText:
        cipher=ord(x)+distance
        if cipher>ord("z"):
            cipher=(cipher-ord("z")) + (ord("a")-1)
        cipherText+=chr(cipher)
    #output
    print("\nThe encrypted form for",plainText,"is: ",cipherText)
    return cipherText
```

Figure 11. A python encryption function



```
#decryption function
def decrypt(cipherText):
    print("\nDecrypting one word lower case with Caesar Cypher.")
    decode=""
    for x in cipherText:
        decipher=ord(x)-distance
        if decipher<ord("a"):
            wrap=ord("a")-decipher
            decipher=(ord("z")+1)-wrap
        decode+=chr(decipher)
    #output
    print("The decrypted form for",cipherText,"is:",plainText)
```

Figure 12. A python decryption function



```
Caesar Cypher Encryption and Decryption.
Enter your text to be Encrypted (one word lower case text): security
Enter the distance: 3

The encrypted form for "security" is:  vhfxulwb

Decrypting one word lower case with Caesar Cypher.
The decrypted form for "vhfxulwb" is: security

Program Run Date and Time:  Tue Feb 25 05:05:09 2020

Thank you for using this program.
Press Enter Key to exit the program or any other key to run the Program again: a
_______________________________________________________________________________

Caesar Cypher Encryption and Decryption.
Enter your text to be Encrypted (one word lower case text): malware
Enter the distance: 2

The encrypted form for "malware" is:  ocnyctg

Decrypting one word lower case with Caesar Cypher.
The decrypted form for "ocnyctg" is: malware

Program Run Date and Time:  Tue Feb 25 05:05:19 2020

Thank you for using this program.
Press Enter Key to exit the program or any other key to run the Program again: s
_______________________________________________________________________________

Caesar Cypher Encryption and Decryption.
Enter your text to be Encrypted (one word lower case text): privacy
Enter the distance: 4

The encrypted form for "privacy" is:  tvmzegc

Decrypting one word lower case with Caesar Cypher.
The decrypted form for "tvmzegc" is: privacy

Program Run Date and Time:  Tue Feb 25 05:05:32 2020

Thank you for using this program.
Press Enter Key to exit the program or any other key to run the Program again:
_______________________________________________________________________________

Goodbye!
>>> 
```

Figure 13. A python Caesar cipher encryption and decryption example results