A DIVE INTO CYBERSECURITY

Author:
Chuqi Zhang
University of Central Missouri
March 2022

Abstract

Today, more businesses are moving their data, business plans, and even their sales online. With this, there are many security risks that come with the convenience the Internet provides. The biggest question of concern is how to keep our data safe. Whether it is the information of the business, confidential data of competitive advantages, or personal data of the customers, keeping the online data safe is a priority for many industries. With online interactions, online attacks which are known as cyberattacks are on the rise and attacks can include the hacking of a system, phishing emails, or unauthorized access to company computers. In 2020 alone, cyberattacks were estimated to have caused around one trillion dollars to the global economy and over 30 billion records have been exposed due to data breaches and those numbers are still on the rise. With current risks and attacks, there are numerous ways to prevent and counter the attacks. Businesses are building firewalls on company systems and are putting in a series of protective measures such as antivirus programs and software in hopes of detecting the malicious attacks at an early stage. Even with preventative measures, attackers are finding their way around firewalls and the protections and are coming up with different ways to attack businesses each day. With new attacks and preventative systems being modified constantly, cybersecurity is a consistent battle that is being fought every single day across the globe.

History of Cybersecurity

The idea of a computer virus was first predicted by a mathematician in the late 1940's but it was not until 1971 that the first creeper worm, a type of computer virus, was created and used to spread to systems to display messages as an experimental self-replicating program (Matthews, *n.d.*). At this time, cybersecurity was not the topic of the headlines in everyday life compared to today where cybersecurity is a top priority for every organization. For the majority of the 1970s and 1980s, many of the threats were from malicious insiders who gained access to documents that they should not have access to (Mutune, *n.d.*). With the first creeper worm, it was designed to infect UNIX systems and then replicate itself on machine after machine. As a result, clogged networks were causing the connected systems to crash, and the internet would slow down so much that it would leave untold damage in its wake. With the worm being the first known program to exploit system vulnerabilities, it received full media coverage at the time and the founder, Robert Morris, became the first person to be charged under the Computer Fraud and Abuse Act with a fine of 10,000 dollars, three years of probations, and dismissal from Cornwell (FBI, 2018).

The start of the creeper worm triggered the start of a new field in computer security as it led to more people researching on how they can create deadlier and more effective worms and viruses. This had thus led to the rise of antivirus solutions as a means of countering worms and virus attacks in an effort to protect computer security. Since then, viruses became more aggressive programs starting in the 1990s and new popular viruses were infecting tens of millions of computers that was causing a worldwide failure of email systems. Back then, virus attacks were mainly focused on financial gains or strategic objects. However, the lack of security solutions back then was causing a huge number of unintended victims to be affected across the world and suddenly, cyber threats and attacks became a huge concern in need of an immediate solution (Mutune, *n.d.*).

With the demand came the creation of solutions. Antivirus software solutions became greatly popular as cyber threats and attacks were a great concern. The programs were designed to detect the presence of viruses and prevent the virus from accomplishing the intended task. The early 1990s was the biggest growth of companies creating and retailing antivirus products that would scan computer systems for the presence of malice identities. While there were many improvements in detecting and keeping viruses and worms out, there were still two significant problems that existed in those early antivirus solutions. The problems were mainly involved around the intensive use of resources and a large number of false positives. The intensive use of resources caused the most problems for users as antivirus scanning systems were using up a lot of the available resources that was interrupting normal user activities and productivity. As the number of malware samples produced every day increased, the problem did not go away. As a reference, only a few thousands of malware samples existed in the 1990s while the number had gone up to at least five million by 2007. As a result, older antivirus solutions cannot handle such capacities as professionals were unable to come up with enough signatures to keep up with the problems as they emerged. Thus, even today, the issues persist in some of the current cybersecurity solutions (Mutune, *n.d.*).

Today, there are so many more hacker groups and organized cybercrime groups that cybersecurity is still as important as ever. As of 2020, the average cost of data breaches is sitting at $3.86 million and the worldwide information security market is estimated to reach $170.4 billion dollars in 2022 in efforts to stop malicious attacks (Sobers, 2021). With the recent global pandemic and increase in remote working conditions, businesses and the government are facing the highest pressure in enhancing their cybersecurity strategy and prove to themselves and their customers that data protection is a critical part of their strategy plan. Besides antivirus software and companies putting in their own firewalls and security, the government is also stepping in to further protect systems and confidential data.

Cyberattack Motives

There are quite a few motives that drive cyberattacks. The ones most related to businesses are financial and intelligence gathering. Recently, about 76 percent of breaches are financially motivated as there is a huge increase in ransomware, attackers entering the organization’s systems to take control, sending alerts to users, or to notify them of the attack until receipt of a ransom fee. With intelligence gathering, cybercriminals are leveraging the practice of scanning, monitoring, collecting, and extracting sensitive information from businesses in order to extort, blackmail, or gain advantages over rivals (Dell Technologies, 2019). In the cyberattack world, motives also categorize cyberattacks into different groups. While most of the cyberattack motives are due to intention of harm to the business or of some type of personal gain, there are also attackers who work in favor of the companies in order to develop antivirus software or to stop active attacks. The most known hackers are categorized and shown in Table 1.

Table 1. ***Types of Hackers and Their Intentions***

Hacker Categories	Intent of the Hackers	Example
Black Hat Hacker	Mostly cybercriminals hacking systems with a malicious intent for their own personal gain.	Hackers infiltrating a company’s security system to access and steal the private personal data of the customers.
White Hat Hacker	These are cybersecurity experts that utilize their knowledge to help prevent malicious cybersecurity attacks.	Security experts hired by a company to specifically research and develop malware detection in order to prevent malicious attacks.
Grey Hat Hacker	Grey Hats are similar to Black Hats in their interest of finding gaps in different systems to break into but without the malicious intent of those under the Black Hat category.	An unauthorized hacker purposely hacking into a company’s platform as a challenge for themselves and utilizes the opportunity to notify the company of the loophole that needs correcting. While they would’ve violated the company’s policies, no harm was caused.

(Rafter, 2022)

Types of Cyberattacks

The most common type of cyberattacks would be with malwares which is the deployment of malicious software, including ransomware, spyware, viruses, and worms to infect and breach a network. With data shown in 2020, the average ransomware payments have increased by 33% over the year 2019 to $111,605 and the average cost of an attack on businesses is expected to cost $133,000 (Sobers, 2021). Attackers can also perform snooping online as they gain unauthorized access to systems and data. There is also data integrity which is malicious data manipulation of a business. Many of the cyberattack methods are difficult to detect and could exist within a business's system for months at a time. Being aware of the different types of cyberattacks can help a business in detecting abnormal activities and detect attacks early on (Dell Technologies, 2019). Other types of common cyber-attacks include fake log-in schemes, hacking, keylogging, and phishing. These attacks are targeted towards employees when attackers gain unauthorized access to work computers or when victims are tricked or tempted to enter or respond with personal or work information (Enterprise Nation, 2020). With attacks on rise in 2021, cyber attacks on small businesses are experiencing much more malicious attacks such as web-based attacks with 49%, phishing and social engineering at 43%, general malware at 35%, SQL injection at 26%, compromised and stolen devices at 25%, denial of services at 21%, advance malware at 14%, malicious insider with 13%, cross-site scripting at 11%, ransomware at 2%, and everything else grouped together with 1% as shown in Figure 1 (Purplesec, 2021).

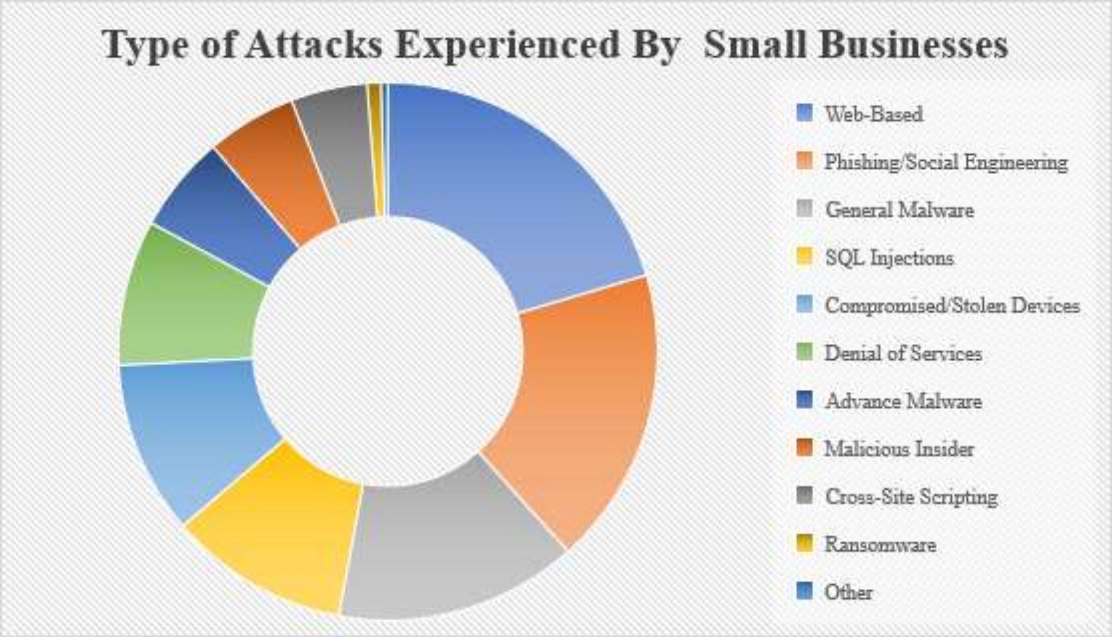

Figure 1

Effects of Cyber Attacks

Cybercrimes can have so many different effects on the economy and within manufacturing. It could impact businesses up to millions of dollars in loss or have companies lose valuable data to outsiders. With businesses storing more of their and customers' data online now, businesses are much more vulnerable to cyber thieves. If cyberattacks succeed, companies are greatly affected, and if cyberattacks fail due to companies' cybersecurity, businesses are paying higher prices in the security of their online data (Investopedia, 2021). Per the IBM report of 2021, the average cost of a major data breach among companies is known to have reached $4.24 million per incident, which has been the highest in 17 years (IBM, 2021). A summarized list of cyberattack impacts is shown in Table 2.

Lost Revenue - The most direct and the worst outcomes of a cyberattack would be the sudden decrease in revenue as consumers become worried for their own online safety and become more cautious to protect themselves from cybercrimes (Investopedia, 2021). Businesses also start losing money internally as they slow their production and work to block attackers and to increase online security. Globally, losses from cybercrimes are totaling over one trillion dollars which was more than fifty percent increase from data in 2018. Companies are reporting much more cyber incidents now and the average cost was more than half a million dollars per incident (Businesswire, *n.d.*).

Operational Disruption - Besides financial damages, companies often face operational disruptions when cyberattacks happen, thus causing the increase in indirect costs for businesses. When attacks happen online, there is a great possibility for major interruptions of the manufacturing operations as security work on defending the systems and ensuring data is safe and operation is good to proceed. Often, the use of viruses and worms can cause a company's internal website to malfunction or completely shut down. This also causes operations to be at a standstill and can be very costly and time-consuming to fix. This often results in lost revenue and a decrease in productivity (Kaput, *n.d.*). Data in the past couple of years are showing average interruptions to operations to be around eighteen hours on top of manufacturing downtime and reduced efficiency (Businesswire, *n.d.*).

Reputational Damage - When it comes to the internet, information can never be erased once it is leaked. So unlike lost revenue and operations disruptions where the companies can work to recover from the losses, reputational damage is something that can never be fully recovered. Once confidential information is leaked, the business not only loses important data and competitive advantages, but they will also lose the trust of their customers as their brand image becomes damaged. With customer loyalty, it is a negative effect that includes loss in customers and even potential lawsuits. Even with confidential information that was lost then restored, there is still a great risk of data being exposed to the public that can never be reversed (Clickatell, 2017).

Stolen Intellectual Property - Another effect of cyberattacks is the risk of intellectual property being damaged. Once a system is infiltrated, company ideas, marketing campaigns, or business expansion plans all become exposed, and the company would lose all competitive advantage over their competitors. It will be so easy for cybercriminals to steal the ideas and plans to be sold or exposed to other businesses or on online platforms, making them useless and costly as the company loses years of valuable work. This also damages future business growth and revenue gains as intellectual property gets stolen (Pribanic, 2018).

Altered Business Practices - After each cyberattack, businesses are impacted in other ways too. Companies will have to rethink how to collect and store information in the future to ensure online safety and many companies will have to stop storing customer financial and personal information online until a secure system is in place. Worse, some companies might face shutting down their online stores due to concerns of cyberattacks until they can adequately protect themselves. Businesses will also owe customers new business plans on how security issues are being dealt with and the protections to be installed to ensure the safety of all the data information (Investopedia, 2021).

Increased Costs - Post cyberattacks, companies will be the most focused on how to protect themselves from online thieves. To do so, businesses will have to increase cybersecurity technology and expertise, notify affected parties of such a breach, and to investigate insurance and legal support. In order to better protect the business, they will have to pay more for the business to succeed in online security. Businesses will have to hire security experts and lawyers to deal with the attacks and remain in compliance with cybersecurity regulations. If the attack is a ransomware, it could also create a major financial burden as hackers often ask for large sums of money to be wired. There could also be increased cost in attorney fees and damages for the companies if the attacks are successful and customer data are lost (Investopedia, 2021). Overall, online attacks can affect a business directly to profit and indirectly with halted production, increase in online security, and also costs to resolve the damages of the attack.

Table 2. ***Effects of Cyber Attacks***

Lost Revenue

- Sudden decrease in revenue as customers worry for their online safety
- Business slow production/work to block attackers causing delay in service/product deliveries
- Globally, losses from cybercrimes are totaling over one trillion dollars

Operational Disruption

- Major interruptions of the manufacturing operations
- Operations being at a standstill can be very costly and time-consuming to fix
- Data shows an average interruption to operations to be around 18+ hours

Reputational Damage

- If data is leaked online, it can never be erased
- Loss of customers and potential lawsuits.
- Reputational damage of the company can't be fully recovered

Stolen Intellectual Property

- Company ideas/marketing campaigns/business expansion plans become exposed
- Companies will lose their important data and competitive advantages.
- Easy for cybercriminals to steal the ideas/plans to be sold/exposed to other businesses
- Damage future business growth and revenue gains as intellectual property gets stolen

Altered Business Practices

- Rethink how to collect and store information to ensure online safety
- Stop storing customer financial/personal information online until a secure system is in place
- Businesses face shutting down due to cyberattack concerns
- New business plans required to resolve security issues and installation of system protection

Increased Costs

- Increase in cost to obtain better online security and hire technology/security experts
- Cost in working with lawyers/insurance
- If the attack is a ransomware, it could also create a major financial burden
- If the attacks are successful or customer data are lost, compensation would be high

Examples of Successful Cyber Attacks and Effects

While cyberattacks seem so far away in context, it actually happens daily globally. In 2021 alone, there were 1,862 reported data breaches in the United States, which is a 68% jump from previous years (Fowler, 2022). Even with major security in place, companies are still being targeted by hackers with malicious intent. Even some of the biggest companies in America have endured some type of cyberattack in the last couple of decades. Here's a few examples of successful brands that have had security breaches in the past. In June of 2021, Volkswagen revealed a data breach that impacted over 3.3 million customers and buyers in North America. Per the automaker, there was a compilation of data purposed for sales and marketing between 2014 and 2019 that was left unsecured and exposed online sometime between August 2019 and May 2021. Audi and Volkswagen were alerted of the unauthorized third party accessing the information in March of 2021 and that person information such as name, mailing addresses, email addresses, phone numbers, driver's license, social security number and vehicle information associated with those people has been exposed (Spicer, 2021).

Another well known cyber attack in 2021 was the Colonial Pipeline ransomware attack that happened in May of 2021. With the Colonial Pipeline being one of the largest and most vital oil pipelines in the United States, a hacker group identified as DarkSide accessed the Colonial Pipeline network and stole 100 gigabytes of data within a two-hour window. With the data in hand, the attackers infected the IT network with ransomware that affected many of the company's computer systems, including billing and accounting. Due to the attack, Colonial Pipeline was forced to shut down the pipelines to prevent the spread of the ransomware, causing days of shutdowns impacting the supply of oil from refineries to industry markets which caused the president to declare a state of emergency. Due to the attack, the company involved the FBI, Cybersecurity and Infrastructure Security Agency, U.S. Department of Energy, and Department of Homeland Security in an effort to stop the attack. After a week of shutdowns, Colonial Pipeline was forced to pay roughly $4.4 million in bitcoins to the hackers in order to restart the pipeline and resume normal operations. A month later, the Department of Justice was only able to recover approximately $2.3 million in bitcoins from the attackers (Kerner, 2021).

Current Solutions and Defense Mechanisms

With so many hacker groups and organized cyber-crimes today, there are also many improved solutions and defense mechanisms preventing and stopping cyberattacks. The first solution to prevent cyberattacks is to have a secure and sophisticated hardware that is password protected and backed up by 2-way authentication (Goud, *n.d.*). It is also important to safeguard the company's hardware as it is very dangerous if data breaches occur when stolen equipment reaches the hackers. Thus, any physical security strategies or safeguards within the equipment systems are important to have protection by multiple security layers. Encryption is also essential to protecting company data. By encrypting data, it gives the company a better chance of not losing important data when it lands into wrong hands. Sometimes, even with all the defense mechanisms, hackers will still be able to infiltrate the networks and try to encrypt the data with ransomware. Thus, it becomes much more important to have a backup data file on hand. When situations like this happen, backed up data allows the company not to bow to the demands of the attacker and also have an upper hand in negotiations (Goud, *n.d.*).

When it comes to blocking malicious attacks, anti-malware solutions would be a great investment for the business. Whether it is the use of firewalls, antivirus software, or applications that detects malicious content, it is important for companies to be prepared and have sufficient protection in place. By monitoring the IT environment to uncover vulnerabilities and addressing them before attacks happen is one of the best means to achieve optimum security. Today, there are a large number of cybersecurity tools such as Wireshark to test network security, Netstumbler for network defense, and TrueCrypt for encryption (Mutune, 2021). There are hundreds of anti-malwares for businesses to choose from based on the category of need and there are also lots of cybersecurity experts that can assist businesses in the security of their online data. With those companies that choose to install some sort of antivirus programs or software, at least 350,000 pieces of malwares are being detected each day in the United States (Jovanovic, 2022).

To ensure the protection of the company's systems, the risks must be taken seriously from the beginning. With the ever-growing cyber threats, the potential cyberattacks should be communicated across board and be made widely known across the business. Companies should be talking about the importance of security at board meetings, everyday meetings, and management should set the tone and culture of security mindedness within the organization (Mimecast, *n.d.*). Doing so will not only raise awareness of the importance of cybersecurity but it will remind employees to be on the lookout for potential threats every day. With this, it is also important to develop a cybersecurity strategy for the organization. Companies must do internal research first to identify the specific threats that the business faces and include complete audits of current security tools, training programs, and security practices. Such activities can help identify the specific cybersecurity needed for the organization and ensure the current plan in effect meets the guidelines and requirements of the company (Mimecast, *n.d.*).

With cybersecurity becoming more important nowadays, it might also be wise to invest in cybersecurity insurance. This is designed to mitigate losses from different cyber incidents such as data breaches, business interruptions, and network damages. With cybersecurity insurance, it can assist in the reduction of successful attacks by promoting the adoption of preventative measures in return for more coverage and encourage the implementation of best practices by basing premiums on an insured's level of self-protection (Cybersecurity & Infrastructure Security Agency, *n.d.*). With the thought that even the most advanced cyber defenses can be broken into, cyber insurance can cover financial losses and assist in the co-paying of the costs involved to recover data including paying data recovery experts and purchasing of new hardware and software (Goud, *n.d.*).

Lastly, cybersecurity training is another important factor when it comes to cyberattacks. Educating employees can help mitigate cyber risks as it teaches employees how unsecured networks can access work information that could put sensitive data at risk. By providing training, it allows employees to better recognize, report, and eliminate security threats. Today, many security breaches happen through employees and they are the most common entry points for phishers and attackers. Cybersecurity training not only helps employees recognize the effects of a cyberattack, but it can also help protect themselves and the company against potential threats. By making employees able to identify and eliminate cyber threats, the company is strengthening the most vulnerable link in the chain and reducing the risk of cyberattacks (Ramachandran, 2019).

Recommendations

For any business, the first action to take is to ensure the sufficient use of password management. Adopting effective password management is the key to protecting business data and avoiding risks within the company. Despite passwords being the easiest way of maintaining website security, it is also the highest security risk if not managed properly. As a manager, it will be crucial to stress the importance of password protection to the team and practice top password security (Mutune, 2021). **I**t is also strongly encouraged to have employees encrypt their work and their confidential emails to ensure only intended receivers are seeing private company information.

Next, training is the key to educating the team and teaching everyone how to detect and protect themselves and the company when it comes to cyberattacks. Training should not only happen at the beginning of an employee's onboarding, but it should be a recurring training to remind employees of their roles in the business. Classes should include how to detect different types of attacks such as phishing or unauthorized users and teach employees what to do when something abnormal is detected. Internal testing can be used such as sending out controlled phishing emails to employees to raise awareness and keep everyone alert on the fact that anyone could experience a security breach and the importance of reporting those incidents.

Once employees are training and password protection is perfected, management should take a look at companywide regulations. Whether it is the requirement of data backup or the use of antivirus technology, managers should do their best to follow company guidelines and ensure no malicious attacks can make it pass the first line of defense.

Summary

As more work is being done online today, the need for cybersecurity is at an all time high. What started in the 1970's as a worm to send a small message across systems have now become ways for hackers to make money and sell private company information. It is creating losses of profit, productivity, and customer loyalty as more cybersecurity breaches happen. However, with more attacks, more defenses are being put in place such as firewalls or antivirus applications to detect and protect the systems from cyberattacks. Table 3 shows a summary of the different types of common attacks and the ways to prevent or stop the malicious attacks.

Table 3. ***Summary of Cyberattacks and Prevention Methods***

Phishing	Malicious actor sending emails that seems to be trustworthy and legitimate in hope of the receiver being fished to click on malicious links	Training and internal phishing tests to keep employees on high alert and avoid opening any emails that look suspicious
Ransomware	Victim's system gets hacked and will be held hostage until a ransom is paid to the attacker	Companies should always maintain backups, keep systems up to date, and provide security awareness trainings to employees
DoS (Denial-of-Service)	Attackers will hack into a system and overwhelm the resources with illegitimate requests until it is unable to respond to actual legitimate service requests	Best prevention effort would be the use of firewalls to detect intrusions and stop those malicious requests along with strengthening security systems with antivirus software
Password Attack	Attackers can intercept network transmissions in order to obtain passwords that are not encrypted or use social engineering to convince targets to resolve an "at risk" situation by entering in their passwords	Training should be provided to employees at a consistent basis and businesses should encourage the use of encrypted passwords or implement lock-out policies on company systems
Structured Query Language (SQL) Injection	Hackers will use an SQL query to inject a command into a data plane replacing something that would normally be in place. Once the hack is successful, SQL can allow the hacker to have access to credentials/data and they can also alter/delete records and data in the	Manage the company on a "need-to-know" basis and only allow those who have a need for the data to have full access. Companies can also incorporate validation and queries in place to filter out invalid accesses. The use of firewalls and antivirus software can also be useful in the scanning/detection

	database	
Insider Threats	These are people within a company that have access to systems and privileges that can put the organization at risk	Companies should be implementing security software to detect malicious actions/misuse and perform company-wide risk assessments on a regular basis
Trojan Horse	Malicious programs that are hidden inside another program that seems legitimate – malware inside the trojan horse will be released when the innocent program is used and this allows an opening for hackers to penetrate the system	Training should be provided to employees to raise awareness of potential cyber attacks and that no one should download/install anything or open attachments unless the source can be verified

References

Businesswire. (n.d.). *New mcfee report estimates global cybercrime losses to exceed $1 trillion.* Retrieved from https://www.businesswire.com/news/home/20201206005011/en/New-McAfee-Report-Estimates-Global-Cybercrime-Losses-to-Exceed-1-Trillion

Cybersecurity & Infrastructure Security Agency. (n.d.). *Cybersecurity insurance.* Retrieved from CISA. https://www.cisa.gov/cybersecurity-insurance

Dell Technologies. (2019). *Cybersecurity context & background.* Retrieved from https://www.delltechnologies.com/content/dam/delltechnologies/assets/microsites/connected-cybersecurity/dell_cybersecurity_context.pdf

Enterprise Nation. (2020, November 16). *What impact can cyber crime have on your business?* Retrieved from https://www.enterprisenation.com/learn-something/what-impact-can-cyber-crime-have-on-your-business/

FBI. (2018, November 2). *The morris worm. The morris worm 30 years since first major attack on the Internet.* Retrieved from FBI News. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Fowler, B. (2022, January 24). *Data breaches break record in 2021*. Retrieved from Cnet. https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

Goud, N. (n.d.). *Ways to prevent cyber attacks on your company.* Retrieved from Cybersecurity Insiders. https://www.cybersecurity-insiders.com/ways-to-prevent-cyber-attacks-on-your-company/

IBM. (2021). *How much does a data breach cost?* Retrieved from IBM. https://www.ibm.com/security/data-breach

Investopedia. (2021, March 24). *6 ways cybercrime impacts business.* Retrieved from https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx

Jovanovic, B. (2022, March 14). *Virus alert: 31 antivirus statistics and trends.* Retrieved from https://dataprot.net/statistics/antivirus-statistics/

Kaput, M. B. (n.d.). *What can happen to a company as the result of cybercrime?* Retrieved from Chron. https://smallbusiness.chron.com/can-happen-company-result-cybercrime-26811.html

Kerner, S,M. (2021, July 7). *Colonial pipeline hack explained: Everything you need to know.* Retrieved from https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Matthews, T. (n.d.). *A brief history of cybersecurity.* Retrieved from Cybersecurity Insiders. https://www.cybersecurity-insiders.com/a-brief-history-of-cybersecurity/

Mimecast. (n.d.). *Best practices for cyber security defenses.* Retrieved from https://www.mimecast.com/content/protecting-data-in-the-healthcare-industry/best-practices-for-cyber-security-defenses/

Mutune, G. (2021). *27 top cybersecurity tools for 2021.* Retrieved from Cyberexperts. https://cyberexperts.com/cybersecurity-tools/

Mutune, G. (2021). *Top 12 website security practices for 2021.* Retrieved from Cyberexperts. https://cyberexperts.com/website-security-practices/

Mutune, G. (n.d.). *The quick and dirty history of cybersecurity.* Retrieved from Cyberexperts. https://cyberexperts.com/history-of-cybersecurity/

Pribanic, E. (2018, May 25). *Impact of cybercrime on business.* Retrieved from Tech Funnel. https://www.techfunnel.com/information-technology/impact-of-cybercrime-on-business/

Purplesec. (2021). *2021 Cyber security statistics. The ultimate list of stats, data & trends.* Retrieved from https://purplesec.us/resources/cyber-security-statistics/

Rafter, D. (2022, February, 25). *What is the difference between black, white and gray hat hackers?* Retrieved from Norton. https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html

Ramachandran, R. (2019, October 15). *The importance of training: Cybersecurity awareness like a human firewall.* Retrieved from Entrepreneur India. https://www.entrepreneur.com/article/340838

Sobers, R. (2021, March 16). 134 *Cybersecurity statistics and trends for 2021*. Retrieved from Varonis. https://www.varonis.com/blog/cybersecurity-statistics

Spicer, C. (2021, July 9). *Volkswagen data breach exposed 3.3m names, addresses, vins, claims class action lawsuit.* Retrieved from Top Class Actions. https://topclassactions.com/lawsuit-settlements/privacy/data-breach/volkswagen-data-breach-exposed-3-3m-names-addresses-vins-claims-class-action-lawsuit/