A Look into Preventing Cybersecurity Threats in the Evolving World of Digital Applications

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jonathan Wen
Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor
Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction:

Web development is one of the fields of computer science that has gained a lot of traction, with a high demand for full stack computer scientists in many large companies. Full stack implies that programmers are familiar with both frontend development- which includes user interface and webpages, as well as backend development- which includes database and server responses. UVA's courses even tailor towards its students becoming good at both front and backend development. With web development comes the creation of many applications. From social media like Facebook, to banking apps, to messaging and email, people are moving towards a world where all of their personal information will be saved somewhere in the digital world. With this in mind, many people are aware and concerned of the ever-evolving risk of cybersecurity risks. Attacks come in many different forms, ranging from attacks to gain personal information to shutting down a system or site as a whole. In a Forbes article, Tim Cook mentions the immoral choice Facebook makes to compile user data as a selling point for targeted advertising (Dierickx, 1). This is but a small example of how unaware the general population is of how their data is being used. Hackers are becoming more and more creating with the ways that they try to crack systems, as many things like banking and interactions are becoming online. Through methods ranging from targeting unaware victims clicking malicious links to systemic attacks like SQL injections, websites can be susceptible to attacks if not properly protected. Although it's difficult to predict an attack, certain standards need to be met in order to prevent known methods of hacking from succeeding. The current issue with preventing attacks is that hackers will always have the "one step ahead" advantage as they are developing new ways to take advantage of security measures or features to gain what they want. Cybersecurity aims to stop such hackers; however, it is never fully prepared to deal with the new methods that hackers will try to put out. The issue lies in the fact that hackers are developers trying new methods while cybersecurity practices are stagnant with no direction of improvement. With so much personal information on the web, people's livelihood can be at stake if a website, for instance a banking site, is compromised. An example would be the hack on JPMorgan that led to the theft of more than 80 million customer records. Another consequence would be with national security risks, as many hackers have attempted (with some successful cases) to compromise confidential data from the Department of Defense. Hackers have very different intentions, which means that the consequences if left alone are far and wide. Cybersecurity measures need to be researched more so that rather than waiting for attacks to happen, steps can be taken to actively predict the type of attacks hackers will try.

Supporting Arg. 1:

To redefine what is mentioned above, standards for preventative measures need to be set by researching the most common types of cybersecurity threats attacks, and attempting to place countermeasures in an application to prevent such threats from happening. Some of the most common attacks include malwares, which are malicious software that a clueless user may accidentally install. These are usually distributed through suspicious links from fake profiles or hacks on a person's profile (For instance, your friend sends a suspicious message that prompts you to click a link). Similar to this would be phishing, which involves stealing people's information through them clicking a link that may give access to the hacker. Additional potential threats include SQL injections, which aim to gain information or manipulate databases with personal information, and distributed denial of service (DDoS) attacks, which aim to shut down sites by overloading them with traffic.

To give some context into why cybersecurity risks and necessary defense are so prevalent, we need to take a look at the growing influence and reliance society has on technology. Even more specifically; how much personal information is on the web and the fears that people have relative to safety of that information. According to a Department of Homeland Security list, the "threats from this list that Americans fear most are the ones related to cybersecurity." (Araujo,1). The number of people who sign up for social media grows steadily; according to a Statista survey, the number of social media users grew from 2.86 billion worldwide in 2017 to 3.6 billion in 2020, and is expected to grow to over 4.4 billion in 2025. The issue with this lies in the fact that there's a "lack of a consolidated approach to cybersecurity" (Araujo,1), and an assumption from users that their data is automatically safe. A major issue noted by an ActZero article is the fact that cybersecurity breaches are more and more prevalent, especially within mid-market organizations (ActZero, 1). This blog further mentions that a crucial step in preventing these breaches is "continued user education", yet companies choose not to prioritize cybersecurity at board level. Cybersecurity is more than just an issue with a product or service; it becomes a cultural issue as no one denies the harm cyber-attacks cause, yet a majority of people don't know where to start when it comes to preventing them.

From the points mentioned above, it becomes clear that the knowledge gap between users, and the conditions they are signing up for is very wide. We can come to the consensus that decisions on cybersecurity, much like the decisions companies have to make according to the Tim Cook article, are ultimately ethical choices that need to be made in order to preserve the best interest of its users (Dierickx, 1). Companies need to learn how to take steps to better understand cyber threats, and educate their users before more major breaches occur. From other fields conclusions can be drawn about what happens if systems are unprepared for any level of disaster. The effects of Hurricane Katrina are still felt in many communities, and as mentioned in the call to action, a large part was due to a lack of preparedness for a disaster of that level (ASCE, 1). It becomes all the more urgent as more and more individual financial and personal information are becoming available on the internet; some banks like Capitol One don't have physical bank locations anymore, rather individuals have online accounts that they blindly place trust in to have protected.

In order to better understand where to begin in terms of consolidating cybersecurity efforts, data like Verizon's 2019 Data Investigations Breach Report become very important (Verizon, 3).

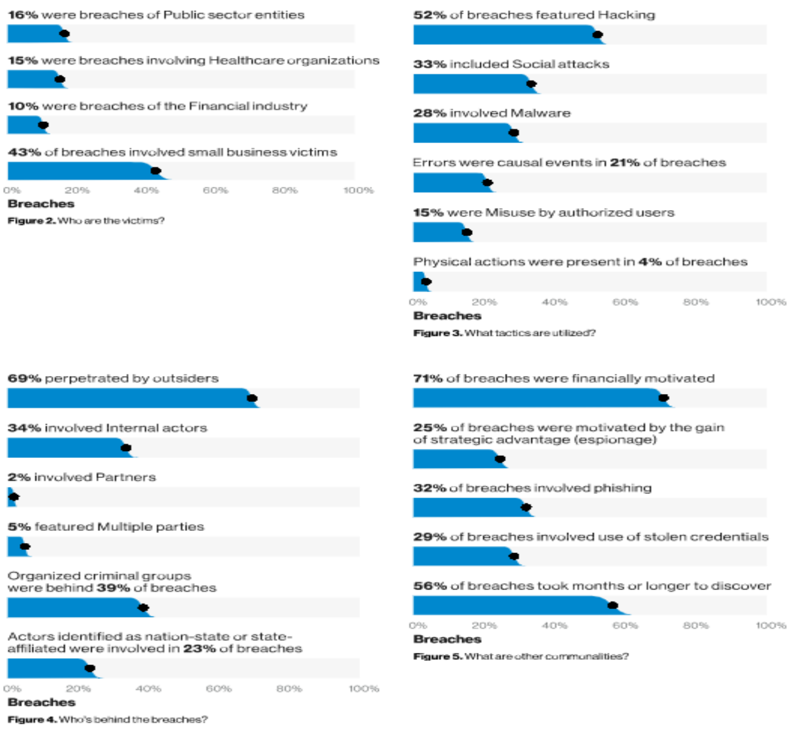
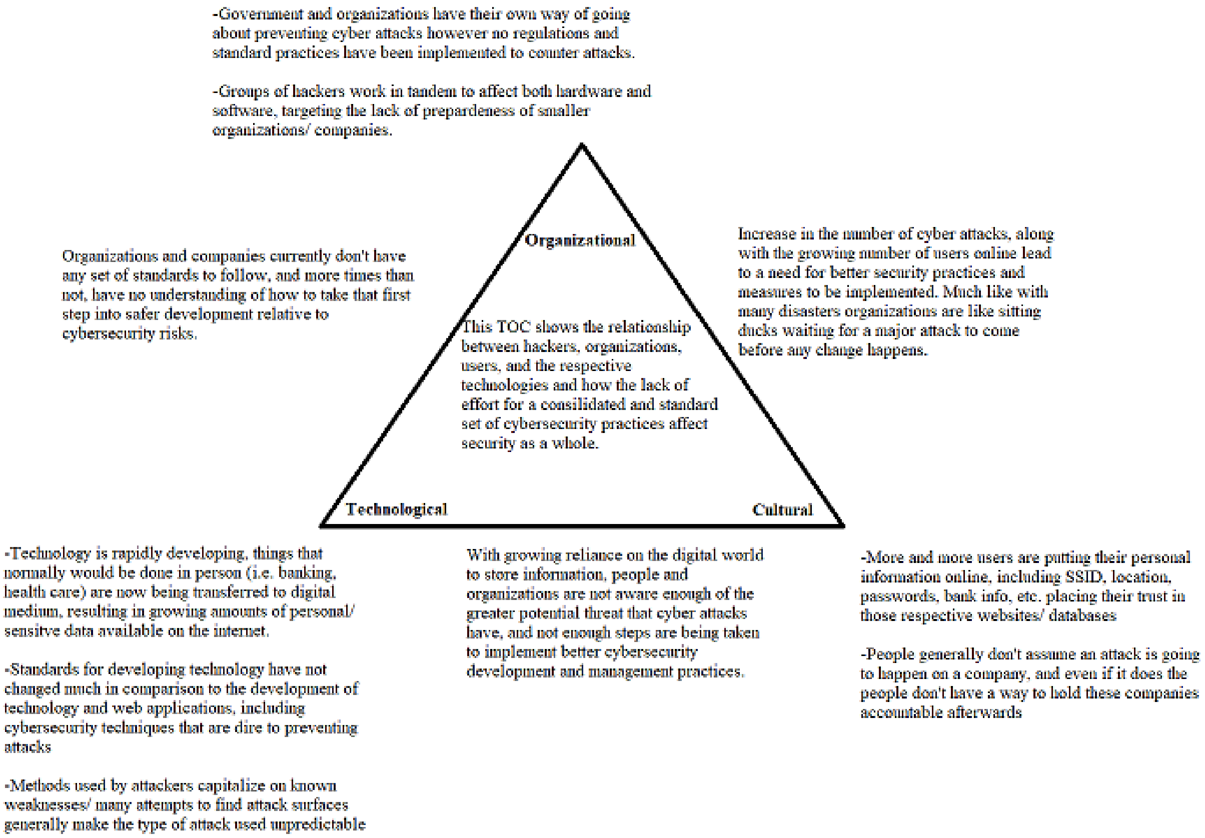


Figure 1: Verizon's 2019 DBIR Summary of Findings

Trends in methods used can become measures of prevention; for instance, 71% of breaches were financially motivated, and 56% of breaches took months or longer to discover. Combining this with facts like 33% of attacks included social hacks show that (like mentioned above) hackers like to target uninformed user through methods like phishing or cross site scripting. From data provided by Lepide (Jefferson, 1), more than 20% of the top 15 most commonly used forms of attack include taking advantage of clueless users by having them click links, or downloading malicious software (methods like phishing, XSS, and malware mentioned above). These statistics can help us develop a starting point on how to better inform users (as well as production companies) on setting a baseline for where to start in terms of tangible first steps on better cyber threat awareness.

By setting some form of expectation on what kind of product is being used, companies can set measures to expect certain kinds of attacks to be used much more often. For instance, a company with high amounts of interaction between users (or interaction between the company's emails and users) can expect the types of attacks to be geared more towards phishing, which requires uninformed/ unaware users to interact with a medium sent by a hacker. Using this information, they can create a way to distinguish identities of real and spam accounts, and also implement some form of verification for official accounts or company users (i.e., a tick). With a first step in mind, it becomes much easier to know how to proceed. Because cybersecurity attack and threats are well documented, it becomes easier for companies to take tangible actions. Next steps can include hiring cybersecurity experts that have the certain requirements needed to prevent the known potential threats.



-Government and organizations have their own way of going about preventing cyber attacks however no regulations and standard practices have been implemented to counter attacks.

-Groups of hackers work in tandem to affect both hardware and software, targeting the lack of prepardeness of smaller organizations/ companies.

Organizations and companies currently don't have any set of standards to follow, and more times than not, have no understanding of how to take that first step into safer development relative to cybersecurity risks.

Increase in the number of cyber attacks, along with the growing number of users online lead to a need for better security practices and measures to be implemented. Much like with many disasters organizations are like sitting ducks waiting for a major attack to come before any change happens.

This TOC shows the relationship between hackers, organizations, users, and the respective technologies and how the lack of effort for a consilidated and standard set of cybersecurity practices affect security as a whole.

-Technology is rapidly developing, things that normally would be done in person (i.e. banking, health care) are now being transferred to digital medium, resulting in growing amounts of personal/ sensitve data available on the internet.

-Standards for developing technology have not changed much in comparison to the development of technology and web applications, including cybersecurity techniques that are dire to preventing attacks

-Methods used by attackers capitalize on known weaknesses/ many attempts to find attack surfaces generally make the type of attack used unpredictable

With growing reliance on the digital world to store information, people and organizations are not aware enough of the greater potential threat that cyber attacks have, and not enough steps are being taken to implement better cybersecurity development and management practices.

-More and more users are putting their personal information online, including SSID, location, passwords, bank info, etc. placing their trust in those respective websites/ databases

-People generally don't assume an attack is going to happen on a company, and even if it does the people don't have a way to hold these companies accountable afterwards

Figure 2: TOC of companies, their users, its technology, and potential hackers.

This TOC diagram condenses the general issues at hand. This diagram essentially states the current standing relationships between hackers, how they affect organizations and what they stand to gain, the lack of preventative measures in place by many (especially smaller) organizations, how digital development needs to change, and how that will ultimately affect the users—the ones most at risk.

Supporting Arg. 2:

As mentioned above, there are so many different types of cybersecurity threats that exist. According to IBM's "Cost of a Data Breach 2020" report based on an interview from 524 breached organizations, it takes an average of 280 days to identify AND contain the breach, costing an average of $3.86 million for said organizations (IBM, 5). The reason for such is because on average only 5% of a company's folders are actually properly protected (Sobers, 1), and the fact that many hackers try to hide their malicious software/ programs.

To get a better look at what steps companies need to make to tighten their cybersecurity sectors, it’s crucial to not only look at different types, but also categorize cyber attacks by intent, or by reaction. To categorize by intent, we must look at potential vulnerabilities involved in a software or service provided. For banks and financial institutions hackers have a large incentive to find ways to deploy malicious software that goes unnoticed and can spread by itself. Methods like cross site scripting or malware are methods in which hackers manipulate unaware users to unintentionally download a malicious software or click a link. These can either let the hackers gain access of a user’s files, or trick the users to input their login information into a false site. One of the biggest hacks that occurred this decade was the attack on the Central Bank of Bangladesh in which “hackers stole $81 million” (Singha, 1). Additionally, a more recent DDOS attack on Hungarian banks/ services is noted to have been one of the largest cyber-attacks Hungary has faced. These statistics are important because they come to emphasize how much more at-risk organizations are as they move to more digital ways of storing data. Again, users need to be aware that security is nowhere near perfect and that they need to be as aware as possible when setting security for their own information and accessing websites.

One of the wider categorizations that cyber-attacks can be split is by is short and long term. Short term cyber-attacks are meant to disrupt an organization or business’s site immediately. This is a very common type of attack that has even affected UVA’s SIS and Collab site logins over the past couple of years. The intention of the hacker can range from stopping a business competitor to political sabotage. On the other end, long term attacks are meant to fly under the radar for as long as possible. These attacks typically operate on a much larger scale, and cost organizations a lot of money and lawsuits to settle. The ways in which these attacks are deployed range in many different ways, however many have the same goal of targeting sites to gather information (i.e., bank information, SSID, etc.) in hopes of leaking it.

As mentioned above, these long-term attacks are likely to result in lawsuits as users lose faith and sue for their personal information being leaked. One of the most notable attacks of such nature was the leaking of over 419 million Facebook user ID’s and (more crucially) phone numbers were discovered to be unprotected by any passwords. This attack rings a lot of ethical similarities to the consequences mentioned in the Katrina call to action article. For starters, we can look at the lack of preparedness of both parties being the inevitable downfall. In our society change is driven by tragedy. Without a tragedy like Hurricane Katrina, the lack of proper defense against natural disasters would never have been brought directly under investigation. People assume they’re safe until they’re not; so, similar to how defenses against natural disasters like Katrina were unprepared, Facebook users would not have expected their personal data to be vulnerable until a leak of such magnitude came to light.

Another similarity between these two cases is the lack of consolidated direction in creating a sufficient defense. The Katrina article stated in the later clauses that professionals need to be brought in and hired to regulate emergency systems with a board of experts to help delegate decisions. Facebook needs to have a level of accountability and better cybersecurity experts, as well as a board to help delegate decisions on how best to protect user data. That becomes even more prevalent with smaller businesses and organizations; Facebook is one of the leading tech companies with software developers that pave the way in innovation in software. Smaller companies may not have as much financial backing to cover for lawsuits and in some cases, the data they need to protect can be much more vital to their user’s wellbeing (medical record or bank account information where if leaked, can cause major damage in one’s life).

As mentioned previously, companies need a way to identify how to take a tangible first step by identifying which parts of their software are at highest risk. The next step from there is to understand the requirements needed to reinforce potential vulnerable attack surfaces. This next step is more ambiguous because there’s so many different fields in which software is used. An attack surface is defined as any part of a software or product that is vulnerable for hackers to attack. For some websites, this could be a non-protected textbox that makes a database vulnerable to SQL injections. For others, it could be a gathering of a response team to respond to sudden volumetric DDOS attacks. The categories of short- and long-term attacks may seem very broad, however the intent behind the attacks do align and thus may allow companies to distinguish what parts of their product/ software are vulnerable.

Supporting Arg. 3:

The bottom line is that there isn’t enough of a cohesive effort to educate company/ organization workers and users about the potential threats that exist. In an ideal world we would have the ability to find and predict attacks and on which surfaces they would occur, however that is impossible due to the simple fact that the development of technology and especially software is growing. Every day new software, new websites, and new coding environments are developed, each with unknown attack surfaces. As mentioned with the Katrina call to action, no one can predict the level of disaster a system will face until that disaster happens. Although organizations may never get to a point where we can predict new types of attacks that would occur, a collection of common steps can be created that these organizations can and should follow in order to minimize the potential cyber threats on software. When it comes to protecting users, a lot is on the line especially when their personal data, financials, and health should be the main ethical priority over anything.

The first recommended step has been mentioned several times above, however it is extremely important to rehash as the most difficult part to overcome in terms of better cybersecurity is the initial identification of potential threats. When a company or organizations adopts new technologies, they need to consider the vulnerabilities that come with it, and how it affects the information they're trying to protect. Hackers have very differing motives and methods of attack based on their intent. A site that stores a lot of user information and uses transactions is definitely going to be a target for hackers with financial gain in mind. Alternatively, if a site is expected to have high traffic (i.e., a shop that releases new inventory on releases) then developers need to be aware that hackers may try to do a direct denial of service attack. Ultimately companies and organizations need to first identify vulnerabilities in order to safely move forward with development and security.

The second recommended step for organizations is to develop a sector dedicated to making decisions on cybersecurity, and working with qualified experts to make the correct ethical decisions. We have to remember that technology doesn't just become a tool when it's released into society. To better understand it's impact we have to treat the technology like an actor as specified in the actor network theory. We must understand that as technology develops and as this product grows, users and hackers' interactions with the product will change as well. Cybersecurity experts need to be around at all stages of development and growth of the application so that attack surfaces will not arise. Throughout history we have seen how ethical decisions and shortcuts for financial or personal gain have caused disasters time and time again. To avoid tragedies on the scale of the Boeing incident, non-biased experts and qualified developers need to be brought in so that all users' information cannot be compromised. We have to remember that tragedy expedites change, and too many major cybersecurity breaches have occurred with little growth in security regulations.

The environment in which an application or software is used heavily revolves around its users. The more users and traffic a site may have, the more likely it is for a percentage of them is unaware of the risks that come with putting their personal information online. From the data provided by IBM and Verizon based on past attacks, we can conclude that some attacks involve the lack of preparedness of users to prevent attacks as well. The third recommended step for better cybersecurity practices is for organizations and companies to implement informative measures in which their users can take to make their site more secure. For social media sites, this could be messages or notifications reminding people not respond to unknown accounts, and to report suspicious users. Otherwise, reminders like passwords with special characters, or alerts that software being downloaded is from an unverified source also need to be more normalized so that those who are not as familiar with technology are at no higher risk.

Like the other steps, what an organization decides to do specifically should be made based on the constraints and vulnerabilities they face. No two products are the same, though they can be similar. The best way to address cybersecurity concerns is to group potential threats and come to a consolidated way to address them.

This last step is more of an encompassing standard slightly touched upon in the second step. Maintenance of security is extremely important as changes in the product can consequently causes changes in vulnerabilities. On all steps listed above an organization's prime responsibility should be to understand how the changes would affect users and their information BEFORE those changes are released.

Many articles are floating around on the internet about what kinds of attacks have occurred, specific technologies one can implement to prevent them, and what sorts of major attacks have happened in the past decade. There is no mention of a level of standard that companies should follow, which is why the steps mentioned above are so important. It may be easy for individuals who work in an organization or users to see potential risks, but to bring those issues to light and to garner change is difficult as many organizations/ companies (that have been on the same standards since their inception) don't have cybersecurity standards imposed. Again, each company has different goals and intentions with their developed software, however the steps above can and should be followed to ensure that user data and website integrity is protected.

Conclusion:

We are inevitably moving towards a more digitized world, and with that comes many threats that have yet to be discovered. Physical breaches have now become cyber, which makes them much harder to discover if a site does not have the necessary breach preventions in place. We are aware of many different types of attacks yet in terms of the developmental process of sites, there aren't any standards set for private businesses/ organizations. With so many users trusting websites and services with their personal information, we cannot let a lack of understanding and shortcuts to compromise their data. We understand that there is no feasible way to predict the types of attacks we may face in the future, as the speed in which technologies are being developed increases. Until an unforeseeable future in which technology plateaus comes, cybersecurity will be behind impending threats. Focuses must instead be set on setting standards for companies and organizations to follow when it comes to protecting user data. Additionally, it lies on such organizations to also inform its users on how to better protect themselves from the malicious software and phishing commonly used by hackers. With the steps listed above organizations and companies can potentially adapt these practices and regulations to tighten the potential attack surfaces.

Of course, there is no perfect way to fully counter all attacks that happen. The responsibility lies on both the users and developers to minimize the risks at hand. If these practices are not implemented then people must be aware that their own livelihood can be at risk. Finally, we also have to understand that if companies and organizations do not take the initiative now to prevent risks, then we will be even further behind in protecting people as software and technology slowly but surely get implemented into all aspects of their lives.

Citations:

ActZero. (n.d.). Cybersecurity knowledge gap: No longer an excuse. Retrieved March 12, 2021, from https://actzero.ai/resources/blog/cybersecurity-knowledge-gap-no-longer-an-excuse/

Araujo, R. (2020, September 13). Growing cybersecurity concerns create opportunity for competitive advantage. Retrieved February 20, 2021, from https://www.securitymagazine.com/articles/93336-growing-cybersecurity-concerns-create-opportunity-for-competitive-advantage

ASCE. (n.d.). Hurricane Katrina: One Year Later. Retrieved February 29, 2021.

Dierickx, C. (2019, February 04). What Tim Cook knows that Facebook doesn't. Retrieved March 15, 2021, from https://www.forbes.com/sites/constancedierickx/2019/02/01/what-time-cook-knows-that-facebook-doesnt/?sh=494658b1a2af

Dobran, B. (2018, September 10). 7 proven tactics to prevent DDOS Attacks. Retrieved February 20, 2021, from https://phoenixnap.com/blog/prevent-ddos-attacks

IBM. (202). Cost of a Data Breach Report. Retrieved March 5, 2021, from https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

Jefferson, B. (2021, March 25). The 15 most common types of cyber-attacks. Retrieved March 5, 2021, from https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/

Minahan, B. (2019, November 1). Effects of cyber-attacks on businesses. Retrieved March 10, 2021, from https://www.anetworks.com/effects-of-cyber-attacks-on-business/

Scarfone, K., Benigni, D., & Grance, T. (n.d.). Cyber Security Standards. Retrieved March 5, 2021, from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153

Singha, R. (2020, December 19). Banking industry faces surge in cyber security challenges. Retrieved March 19, 2021, from https://securityboulevard.com/2020/12/banking-industry-faces-surge-in-cyber-security-challenges/

Sobers, R. (2021, March 16). 134 cybersecurity statistics and trends For 2021: Varonis. Retrieved February 29, 2021, from https://www.varonis.com/blog/cybersecurity-statistics/

Swinhoe, D. (2021, January 08). The 15 biggest data breaches of the 21st century. Retrieved March 4, 2021, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Tankovska, H. (2021, January 28). Number of social media Users 2025. Retrieved March 1, 2021, from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Verizon. (2019). 2019 DBIR summary of findings. Retrieved March 1, 2021, from https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

Winder, D. (2019, September 05). Unsecured Facebook Databases leak data of 419 million users. Retrieved March 12, 2021, from https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/?sh=734e4a241ab7