**Mission Statement**

With the increasing dependence on digital systems, cybersecurity is in high demand to secure resources, information, platforms, and identities throughout an organization’s entire technical stack, including online and on-prem systems. Public awareness of the need for security and privacy is on the rise, but companies and government regulations are not keeping pace with the fast-changing threat ecosystem. Out of the multiple causes for data breaches, neglect and lack of responsibility from the company on their cybersecurity practices leads the way; cybersecurity is, by nature, a complex field, and a lot of companies have trouble keeping up with its ever-changing landscape. In particular, hierarchy communication inside of small and medium companies make it hard for professionals to procure the actions they need to secure their assets. Technicians have issues communicating the importance of the change to their superiors, or administrators lack the personnel with the adequate knowledge on implementing the changes they need.

Businesses have responsibility over their customers, just as customers have rights that should be respected. With the lack of regulation and explosive growth of the tech industry, the safety and quality standards that are normalized in other industries have failed to be implemented or translated into digital technology. Business practices, in general, strive to be aligned with ethics; without a measure or rules, there’s no room for accountability, and so little ground for ethical practices to evolve. In particular, beyond ethics but within rights, customers do not have the opportunity to hold companies accountable for their mistakes and mishaps when dealing with their own personal information, and businesses do not have a clear north on what to do or how to improve their security, either for their own gain or for the responsibility they have to their customers.

The goal of this project is to bridge the communication gap between administrative and technical positions by enumerating and exploring the concrete ways companies’ security practices can be aligned with current best practices for consumer data protection. Drawing from expectations implied by U.S. state, federal and international law (such as the California Privacy Act, HIPAA and EUGDPR), industry standards and current understanding of effective IT security practice, the guideline developed in this research shows the actions that companies should follow in order to secure their customers’ data and by extent achieve an ethical business practice as well as the grounds to be held accountable for their actions and mistakes. This is all focused from a business perspective: security is approached in terms of a ‘calculated risk’ and the acceptance of consequences instead of the traditional technical-only analysis, which is often incomprehensible to management.

This project will be implemented in two phases: research and implementation. Research is done through the present class (CAPA Advanced Workshop), showing the importance and relevance of why should companies be held accountable for their practices. Implementation is done through a tutorial (CS Advanced Work), where the explored concepts in the research take the form of a two-version guideline for professionals and administrators in the industry.

**Research**

After a series of data breaches, hacks, foreign interferences and whistleblowers, the world is coming to realize how much it needs cybersecurity, for purposes as simple as creating a Facebook account and as complex as bank transactions on a global scale. Given the incredible dependency on digital technology, the need to secure electronic assets permates most aspects of our lives, from access to food, water and medicine to travel and monetary transactions. Tech companies supply many of the tools used by modern industries to complete their work, ranging from ICS (Industrial Control Software) in factories and plants to CMS (Content Management Software) for websites and public communications. However, given the explosive growth of the tech industry, the safeguards we are used to and have implemented for other industries have not been translated into their digital equivalents. Essentially, tech is the ‘wild west’, where companies can do what they want, how they want. Where other industries have overreached and have been limited by regulations, there is no action in sight from the government or international organizations to limit them. Where monopolies have been broken in the past and non-trusts have been issued, they are now embraced, with the pretext of economic growth. The monetization of private data was seen as first as something innocuous, similar to on-the-street surveys, with the thought that people could do what they wanted with their information. But what this simplistic comparison failed to include is the disproportion between traditional media and digital information, the operations and analysis possible through them, and the possibility of surveillance and correlation through them. Tasks that would take a great quantity of time, people and paper, could be done in minutes by computers. As individuals, we understand the vast difference in digital and traditional media; as part of a system, we fail to acknowledge the consequences or ramifications of the things we take for granted, and the deep changes the media brings.

When we interact with digital technology, be it social media or banking, we tend to think it translates neatly into traditional media. There is no fear in posting information in social media, in the same way that they are comfortable talking about themselves in conversation. But where physical conversations are limited to a space and a receiver, digital records are almost immortal due to their replicable nature. If a physical document is destroyed, it’s certainly gone. If a digital document is deleted, there are ways to recreate it, to rescue it from the disk, to revert the process. Privacy and secrecy are luxuries that not many can afford to keep, in the fear of being isolated from peers and connections that can be maintained through just a bit of sharing. However, all of the information, what is not remembered sharing, what was never shared in the first place, lives somewhere; if it all lives in the same place - or on a place that interested parties can freely access - what stops the stakeholders from misusing it? Because of the lack of understanding of the implications of digital media, the absence of restraint from developers and the ignorance of state actors, digital technology evolved from sharing information to being mined and scoured for everything and anything that can be of interest to third parties. Economic interests and practices justified the creation of a surveillance state in favor of private companies. Governments turn a blind eye, as this benefits them: if a company can determine where and when someone was in a particular situation, and the state can get that information free from the company, why would they stop it?

Today, tailored ads and tracking software are common in web pages and applications. Concerns are being raised over wearable technology and the intimate information they gather, as well as how this information is misused by the insurance industry. Algorithms are used to determine who is worthy of loans, or credit, or promotions. Taking it a step further -- how long will it take for a program to be able to ‘determine’ how likely someone is of committing a crime? What if this determines what opportunities they will get? The bias in computation and programming is well known and discussed, and there is little to no progress on how to decrease it.

This is all possible due to information misuse. Either from inside or outside parties, the way data is approached is a telltale mark on how it can be used for purposes beyond their initial conception. This is muddled by companies that want information for purposes beyond their business practices, or by companies that are not related to technology, but use it. If a company collects sensitive information with a valid reason, but it fails to properly protect it, it is just as guilty as that which collects this information out of unwitting users for their own purposes. An ethical business practice is just as important as a proper security mindset: for the user it matters not if who tracks them is a company, or a thief, for they suffer in both cases. Accountability and ethics go hand in hand.

In its quest for the first place in technological development the United States has allowed its citizens - and citizens elsewhere - to be subjected to companies’ whims. In the case of tech companies, it does not come in the form of lousy products or high prices, as might be seen in other industries, but rather as the direct oversight and transgression of people’s rights for monetization. Most of big tech has built its business model around the massive recollection and correlation of user data - private or otherwise - without their express consent or knowledge. It was only after Snowden’s leaks in 2013 that the general public became aware of the extent of information that was collected about them, and while some progress has been done from those days, headlines pop up daily about a company engaging in sketchy practices with user data, willingly or by omission.

Little can be done from an inside perspective about giant companies’ handling of data when their business model relies on its monetization; changing this would require changing the whole company, which while incredible tempting, is something that needs to happen with the help of lawmakers and lobbyists. But through education and accessibility, there is plenty to do to help companies be secure for the sake of their customers. Security is hard -- it is costly, has almost (if any) revenue for the company, and requires immense knowledge about software use and misuse. For larger companies with a good budget, this is solved by easily by hiring experienced third parties to handle it for them. But for small and medium companies, whose budget does not always allow for this, a head scratcher ensues when the question on how to ‘be secure’ arises. More often than not, companies are not insecure because they want to be: they just don’t know how to do it.

Beyond the knowledge on how to solve security problems, technicians and administrators inside companies also face their biggest hurdles to get things done: themselves. Communication between technical and non-technical people is famously poor, as the former group tends to go into minute details that the latter group does not understand or care about. In large companies with a developed hierarchy, this is not much of an issue, as middle managers tend to ‘translate’ the details for upper management, who then can make informed decisions. However, in medium and small companies, where there is no middle ground for both parties, it is not uncommon for both parties to pay little attention or not try to understand each other, growing caricaturesque images of what the other one does. This communication gap creates problems for everyone involved: both parties grow frustrated and blame the other one for not allowing them to get things done, the company suffers out of inaction, customers are at risk of compromise, and by consequence, the revenue (actual or potential) of the company suffers.

In this project, I seek to address that gap. Neither party has ill intentions at heart; they are confused, out of their element when dealing with one another, and the other party does not give them the information they need or want to hear. This problem has a clear solution that, while not so easy for each side, from a third-party perspective is easy to supply: give each other the information they want! In order to help each side communicate efficiently and effectively with the other, I intend to build a ‘manual’ with two versions, where each side has all the same topics and subjects, but the contents change according to who is reading it. For example, a technical view of ‘passwords’ will include implementation and cryptographic examples, while the administrative one will include information on how to choose a password, company-wide policies and two-factor authentication explanations. In a hypothetical scenario, Bob (the manager) is in a meeting with Alice (the technician). Alice wants to make two-factor authentication mandatory for everyone, as it is more secure and allows for less chance of compromise; when communication so to Bob, he can only think of the hassle that will entail and can’t understand how would things be compromised if he has a password. Alice pulls out the described manual and goes to the information on two factor authentication for administrators, and gives it to Bob. Here, the process of how compromise happens through human error (rather than technical errors) is described, and he can now understand why Alice’s solution is worth implementing. On the flip side, if Bob knows they have to implement this but when going to Alice she doesn’t know how to do it, he can hand her the technician version, where the examples and information on it helps her in the implementation.

**Images**

See Examples and Cases (folder)

The ‘Examples’ folder includes examples on the type of media that would be included in the manual to help explain concepts and situations.

The ‘Cases’ folder showcases events, situations and actions happening all around in tech, relevant to this project.

**Current News and Views on the Problem**

Both the Information Security and Information Technology community seems to agree on a holistic level that a) there is a notorious shortage in cybersecurity professionals and b) communication in the tech industry is lackluster. This has been going on for decades, and the ‘Wild West’ culture of places like Silicon Valley and hacker culture do little to improve the situation. The biggest strides addressing the communication gap have been done by Open Source projects (such as OWASP), who release guides of several sorts to help people on various levels of the hierarchy, such as project managers, developers, security analysts and managers.

**Public Action**

Centered towards cyber security and policy, this paper’s topic is most suited in places where both are discussed, either together or separate. Given the casual language and nature of this work and its work-in-progress status, a talk and/or presentation seems to be the most adequate medium for public engagement, tied in with a web presence, to be published in my own website, which currently hosts other papers on digital rights. I will submit this work to several cybersecurity conferences’ call for papers/presentations (CFP), such as DEFCON, HOPE, Diana Initiative, BSides, among others that I may find along the way, as there are multiple. As of the time of writing, it was accepted to The Diana Initiative and the Vermont Academy of Arts and Science’s Student Symposium. Information on both can be found in Conferences (folder).

Organizations such as the EFF and ACLU could also be worthwhile contributing to, as the ultimate goal of this work is the preservation of digital rights through regulation. This work also has the potential to work closely with open source projects such as OWASP and the Free Software Foundation, depending on the outcome, development and sources used. In the end, this work might end up licensed under the GNU license to be able to be used and distributed widely.

**Resources and Sources**

See Sources and Materials (folder)