Law & Ethics in Info Security

Zevin Alifi

Table of Contents

Limitations of the Law

A variety of challenges face legal systems in regards to technology. Computers and network connections are a complicated thing, so it can be difficult for legal personnel such as courts or jury to parse new up and coming technological advancements, that is if they are technologically literate at all. it would be unreasonable to expect all of them to be so, which is an issue as sufficient understanding of computers is usually necessary in order to prosecute in the case of computer related crime cases.

You as the prosecutor in a court scenario may be required to be the tech specialist and provide a sufficient explanation to the court as to what the egregious actions imply. This requires not only technical knowledge, but the ability to explain the issue at hand in a way that a regular person can understand. Additionally, advancement of technology presents a problem in regards to the law. There is simply not enough time for the law to catch up with developing technologies. This is perhaps the most important reason why it is important to have an ethical code as far as what is permitted as an organization.

Be aware that jurisdiction is a limiting factor of the law as well, cyber crime can be sourced from completely different countries, and what is considered a crime in your location is different, as is the penalty for the crime being committed. Combined with the territorial restrictions of the individual states in the US, this makes it significantly more difficult to take action against a foreign attacker, even across state lines. The system is optimal for physical crimes, but it complicates the matter when the legal issues involve cyber crime. *For most of history, criminal activities have been mainly local in nature, meaning that the victim, the perpetrator, and the criminal event were all at one location at one point in time. [1]*

There have been attempts to make the web qualify as it's own jurisdiction to separate laws there from laws in the real world, however, this necessitates the commitment of other countries to abide by those rules and come to an agreement of what those rules should be, which will take many years of active communication to accomplish if it is even possible at all. This is compounded by how new internet crime is in the grand scheme of things, which improperly prepares many countries for how to handle it. Until then, Internet Service Providers have been given the responsibility to maintain their own rule set.

Benefits of the Law

With all this being said, there is a silver lining to the issue presented by computer crime on the law. Many regulations created for the real world can be applied to digital crimes with some modification. The law offers protections against cyber crimes in two ways. Crimes that pertain to the physical world that apply to digital landscapes. For example, Fraud or abuse laws require little to no modifications to apply to a digital space.

Even beyond that, progress has been made in regards to configuring legal standards specific to computer crime as well, such as copyright law, penalties for illegitimate possession of passwords and other credentials, and Intentional disruption of digital communication systems. “*Governments and the satellite industry have reacted to the growing problem of interference by applying political pressure on States where interference activities originate” [2]*. These offer room to pursue legal action against attackers with already defined laws, it is important to understand these regulations for your own protection and to ensure your organization does not violate them. Legal actions that can be taken against attackers take the form of lawsuits.

Security Ethics

It is important to distinguish the differences between legality and ethics. Consequences for improper ethical practices are different in some ways and similar in others to ones of the legal variety. Not having a good grasp on ethical practices for your organization can have a negative effect on the reputation you have with the general public, which can affect how lucrative your operations are in turn. Individuals within your organization can also contribute to unethical behavior, so it is crucial to keep all those employed up to a standard. *"For corporations, ethics can also include the framework you develop for what is or isn't acceptable behavior within your organization." [4]* It is important to make sure your organization's ethical code is acceptable to the sensibilities of every day people.

A crucial component of a trusting relationship between business and consumer is authorization. For essential data communications that require the exchange of sensitive information, it is important to make it clear to the end user what is being exchanged and for what purpose it is being used for. This will ensure a level of trust, as the end user is given due disclaimer.

There should be limits to what data can be taken from the end user. Optimally, data that is essential for operations should be the only thing taken from users. You should not give your business the opportunity to spy on people's personal files that are in no way related to your service. As an extension of this same principle, theft of user data is absolutely forbidden. Unknowing or non consensual use of data will negatively effect the assurance the end user has for the organization.

Should sensitive information be required for the objective of the service of customers, improper handling of said data could raise many concerns over the trustworthiness the organization is owed. Improperly storing or securing such information, or holding onto personal data far after it is necessary is a surefire way of opening it up to threats. This should additionally consider the data of former and current employees. Wrongful disclosure of former employees have lead to court in the past.
"Defendant's confidentially obligations survive the termination of employment and shall have no time limit" [3]

Overall, the goal should be to simply be considerate to the reservations of the end user. Be ready to justify the use of their sensitive data and what level of information is required to be taken from them. Much in the same way that organizations should be held to these ethical standards, it is a joint effort between them and the end user to maintain these ethical principles.

Conclusion

The impressive and limitless abilities that internet connected computer technology has granted us is a double edged sword. Connection to different parts of the globe for the purpose of business, boundless communication with the outside world being granted to consumers and organizations alike, even between each other. However, in tandem, it opens many opportunities for malicious actors to attack. The unfortunate fact of the matter is that there is always a vulnerability no matter how secure your organization's network is. For this reason, it is important to understand the limitations that this technology poses on the law as well as how to benefit legally and protect yourself. This, in tandem with having a solid code of ethics, is important for maintaining a fruitful business.

References

[1] Susan W. Brenner. (n.d.). Cybercrime jurisdiction. Cybercrime Jurisdiction | Office of Justice Programs. https://www.ojp.gov/ncjrs/virtual-library/abstracts/cybercrime-jurisdiction

[2] U.S. Naval War College Digital Commons: U.S. naval war college research. Site. (n.d.). https://digital-commons.usnwc.edu/

[3] Hnw. (2021, May 18). Alleged wrongful disclosure of confidential information goes to trial. Hanlon Niemann & Wright Law Firm | New Jersey Attorneys. https://www.hnwlaw.com/2020/07/13/another-case-of-alleged-wrongful-disclosure-of-confidential-information-and-breach-of-contract-goes-to-trial/

[4] U.S Naval War College Digital Commons: U.S. naval war college research. Site(n.d). https://reciprocity.com/the-importance-of-ethics-in-information-security/

Unquoted, but used within research.

https://www.computer.org/csdl/magazine/sp/2017/03/msp2017030003/13rRUILc8dI

https://en.wikibooks.org/wiki/Information_Technology_and_Ethics/

Ethics_for_IT_Professionals#Where_do_Ethics_Come_From%3F