**Option #1: Technology-related Regulations**

Liam Bergerson

CSU - Global

ITS462-1

N. Braun

5/21/23

## Option #1: Technology-related Regulations

In a world where the use of technology is abundant, organizations are constantly at risk of falling victim to a security breach imposed by a threat actor. In order to safely protect against these security breaches, regulations are in place that govern the employees of the organization. One of the most detrimental vulnerabilities imposed on organizations is human error. Humans constantly make mistakes that could jeopardize the organization. To combat that, regulations are in place that govern the use of organizational equipment. In this paper, two regulations related to technology will be discussed along with how these regulations influence how technology is implemented and managed. In order to maintain compliance towards these regulations, an IT audit will be performed to find out if all employees are compliant towards these regulations.

## Regulations and Their Impact on Organizations

As stated before, human error is perhaps one of the most detrimental and most common vulnerabilities towards organizations, the two regulations chosen will be focused on the human error aspect. The HIPAA regulation will govern how employees use organizational equipment when there's sensitive health information on that system. This regulation covers how assets of the organization such as computer equipment, software, networks, computer system accounts and other digital assets are to be used when there is sensitive health information (HCC, 2022). Since these assets are owned by the organization, employees will use these assets as according to the regulation stated by the organization. This

regulation has a huge impact on organizations because employees browse the internet at their leisure. This, however, can result in a security breach. It's important that there are regulations in place to govern how employees safely browse the internet. If employees are completely free to browse the internet as they please, there is a risk that the employee will accidentally install malware on their system which can give a threat actor access to the system and network. The chance of that happening decreases significantly if there is a regulation in place to stop employees from freely browsing the internet. The internet should only be used for work-related purposes when using computers owned by the organization.

The second regulation is the Children's Internet Protection Act (CIPA). This regulation is more focused towards how employees should be enforcing the systems of a library,for example, to ensure children browse the internet safely. It states that there will be certain blocking and filtering measures, monitoring of online activities, measures to block emails to avoid phishing scams (FCC, 2019). All of these will secure the internet habits of children. Phishing scams have a severe impact on organizations. This regulation will block email applications from being used on systems accessible by the public to avoid interacting with suspicious emails. Blocking and filtering measures will ensure that malicious websites are blocked from being visited by children using systems of a library.

## Regulations and Their Influence on Technology Implementation

When implementing computers and smaller devices for employees to use, they need to be implemented with these regulations, when applicable, taken into consideration. The HIPAA regulation and CIPA regulation are crucial when implementing desktops and laptops for employees to use. To ensure that employees use laptops and desktops properly, certain functions may need to be disabled to discourage any usage that is not for work-related purposes. This can be in the form of blocking certain websites that are not work-related. Monitoring software could also be installed into every system to ensure that employees and children are using the devices properly. In terms of compliance, employees must sign a contract if they are to use company devices. That way, if the employee violates any of these regulations, they cannot have an excuse as to why that compliance was not upheld. Admins must also do their due diligence in managing these devices as well. There are many thousands of websites on the internet. Of course, not all websites can be blocked, however, the more irrelevant websites that are blocked, the chance of one of these regulations from being violated decreases.

## IT Audit For Maintaining Compliance

If I were the CIO of this organization that has been impacted by one or both of these regulations, I would proceed with an IT audit in order to ensure compliance is maintained. These regulations are for the safety and protection of clients' sensitive information and that the information must be protected at all

costs. An IT audit centered around these two regulations will help lower the chance of sensitive data being stolen by a security breach due to a phishing scam, for example. Performing an IT audit on the devices that employees use will help determine if the proper measures are in place and that all employees are compliant of these regulations. When using company devices, they should only be used for work-related purposes. Anything other than that should be performed on employees' personal devices disconnected from the company network. Phishing scams are evolving every day to become more believable to victims. These scams attempt to hand over access to the device that is connected to the network to the threat actor. The threat actor can elevate the access of the device in order to gain access to the sensitive data. Compliance to these regulations must be upheld by every employee in order to prevent these types of security breaches from happening. An IT audit to verify compliance and that the proper measures are implemented on each and every company device will help in preventing security breaches from phishing scams.

## Conclusion

HIPAA and CIPA are two regulations that help organizations keep sensitive health information confidential and childrens' internet habits secure. Organizations must do their part in implementing devices and systems with these regulations in mind to prevent sensitive data being stolen from security breaches. An IT audit that verifies the proper security measures are implemented and that all employees are remaining compliant will help secure company devices.

## References

FCC. (2019, December 30). *Children's Internet Protection Act (CIPA)*. Federal Communications Commission. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

HCC. (2022). The HIPAA Privacy Rule. *HHS.gov*. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html