Analyzing the Role of Cybersecurity in Correctional Facilities

Jaysia I. LeeHeung
Old Dominion University

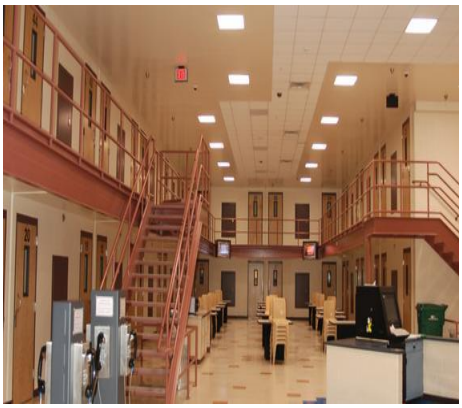
Analyzing The Role of Cybersecurity in Correctional Facilities

Jaysia LeeHueng

Coastal Virginia Center for Cyber Innovation

Old Dominion University

April 12, 2024



Located in Rhode Island, The Donald W. Wyatt detention facility (see Figure 1) went under a ransomware cyberattack in November of 2023. An article read that" The threat group claims to have exfiltrated "Private and personal confidential data, clients' documents, agreements, budget, HR, IDs, tax, finance information, etc." (Schappert, pg.4) Due to Donald W Wyatt being a federal facility, the ransomware attack worried staff as potential inmates may be found guilty due to this cyber-attack even though it is possible, they are innocent. In addition, the facility found that legal documents may be invalidated therefore makes the documents inadmissible in court. Donald W. Wyatt is not the first correctional facility to undergo cyber-attacks. It is important to recognize that society is a part of a digital age that is extremely tech savvy. Due to the emergence of technology, it is imperative to understand how correctional facilities are withstanding digital vulnerabilities. Considering facilities rely heavily on digital infrastructure, tools like radio-frequency identification, inmate tracking, firewalls, security audits, Artificial intelligence, and surveillance, should have high tech security to eliminate any breaches. This analysis explores the significance of cybersecurity in correctional facilities examining the difference between prisons and jails and includes the exploration of how cyber security is evolving with the digital age in these facilities. As correctional facilities embrace the evolution of the digital age, cybersecurity efficacy is in question when protecting inmate information, ethical legal process, and eliminating insider threats.

1. Correctional facilities refer to prisons and Jails

[1] Correctional facilities refer to prisons and Jail

Analyzing The Role of Cybersecurity in Correctional Facilities

The evolution of cybersecurity in correctional facilities

In earlier years knotted ropes were in use to keep inmates in their cells along with wooden locks. As technology progressed, correctional facilities used “simple mechanical locks” (Admin, 2024) Simple mechanical locks were a progressive idea however the locks required physical keys which presented vulnerabilities because the keys could easily be stolen or replicated. Electronic locks “revolutionized the security in prisons” (Admin, 2024) Systems like Biometric locks, and smart locking systems started to be the new norms in prisons. Due to the rapid change in Technology each year, vulnerabilities still can occur. In this case “Cybersecurity threats, system malfunctions and the possibility of unauthorized access are all issues that require constant attention. To ensure the effectiveness of prison lock systems “(Admin, 2024) having updated software systems is imperative when new software is installed. However, many correctional facilities may not receive the funds to install these innovative technologies which initiate breaches in their systems.

Cybersecurity in correctional facilities developed in spurts as location, and available resources varied in different areas. This is one of many examples of cybersecurity in correctional facilities becoming more prominent and useful as institutions started using more computer and network operations.

Technology is used in these correctional facilities to protect inmate information, legal documents, and surveillance of inmates. A major use of technology is the cameras

installed throughout these facilities. Cameras are one of the first forms of technology in these facilities in older facilities, it was found that the cameras did not reach every spot in the facilities and were unreliable. An article “How Updated Video Surveillance Maintains Safety In correctional facilities” Read that “even when caught on camera, the images produced by analog technology are blurry making it impossible to identify anyone but to even find the footage in question, prison staff must sift through hours, days, or weeks' worth of footage to conclude their surveillance system had failed again.”(Staff,2018) This gives hackers more than enough time to go in and obtain legal records and inmate information. Due to the delayed footage, and the slow process of restoration, correctional facilities were at risk for cyber-attacks and breaches.

Types of cybersecurity measures

In correctional facilities vigorous cybersecurity measures are essential when maintaining order, protecting sensitive information, and protecting the overall facility. One relevant measure in correctional facilities is the use of firewalls. Firewalls detect unwanted access that does not align with security requirements. In correctional facilities, firewalls are essential when protecting inmate information, and legal documents. This correlates with access control systems that monitor and control access to data, typically authorized personnel are granted access. Facial recognition systems are up and coming in correctional facilities. An article reads “Facial recognition-powered access control allows officials to effectively manage movement throughout jails and prisons to improve security by controlling which areas prisoners can access” (Oosto,2023).

Artificial Intelligence is another security measure that is up and coming in correctional facilities. An article reads “AI-powered intelligence provides continuous monitoring of the online activities of Security Threat Groups and their co-conspirators" (Wasson, 2023). Artificial intelligence is emerging progressively as “Envisioning prisons in 2030 can hardly be done without the projection of what we know or assume will be available in AI in the future” (Puolakka&Steene, 2021).

Creating a secure digital environment is crucial when implementing new cyber measures. A single overlooked detail could result in a cyber-attack on the facility emphasizing the importance of security audits. Security audits are in place to help” protect critical data, identify security loopholes, create new security policies, and track the effectiveness of security strategies.” (Gillis, 2022) Weaknesses in systems are identified and assets to stop vulnerabilities, security audits may also help create new cybersecurity measures if certain strategies become outdated.

Cybersecurity challenges

Many challenges come with cybersecurity in correctional facilities. Protecting inmate information, legal information, and insider threats all pose significant challenges especially with unique environmental restrictions in facilities.

Protecting inmate information

Protecting inmate information is rigorous because of the amount of information these facilities manage. Not only do they hold inmate information, but there are multiple documents they uphold such as personal information, criminal records, medical records,

and communication records. This makes it easy for hackers to find vulnerabilities because many files could be hacked into. A huge issue the facility is facing is the high turnover rates of staff in these facilities. “For almost 50 percent of corrections agencies, officer turnover rates range from 20 percent to over 30 percent annually” (American Correctional Association, 2023). This is a significant challenge in protecting inmate information because staff members must have proper training to secure this information. Failure of proper training creates an unstable posture for this data protection.

Protecting Legal information

Protecting legal information poses similar challenges as inmate information, but inmates can access it, which poses new challenges for staff. Inmates having access to their information requires additional online monitoring. Encryption data helps regulate sensitive data. However, implementing encryption measures effectively while ensuring access to inmates along with authorized users could be tricky and can lead to leaked information if not installed correctly.

Insider threats

Correctional facilities face huge challenges when dealing with insider threats. Insider threats refer to people who have authorized access to databases and use them to breach operations. Insider threats are extremely broad as they can come from inmates or even staff members. Insider threats are hard to detect as inside operations have full knowledge of the software and may develop loopholes. Spear phishing poses a significant insider threat. A spear phishing attack is when a person tries to steal personal information by using realistic advertisement, this is typically seen through emails. In correctional

facilities, staff members are more likely to indulge in spear phishing due to the amount of sensitive information they have access to. Staff members may also spear phish other employees, by creating realistic emails. This creates a challenge in correctional facilities because system access must be strictly monitored, along with restricted access among different employees.

Is cybersecurity the same in correctional facilities

When using the term correctional facilities, it is important to note there could be a difference between jails and prisons. Although there could be some overlap in protecting inmate information, legal information, and insider threats, some measures may vary due to the differences in facilities. Jails are utilized for inmates who face a short sentence or are awaiting trials, this may cause higher turnover rates which could make it harder to protect inmate information and track legal documents. On the flip slide Prisons are the opposite as their turnover rates are lower because of the longevity of an inmate's prison sentence. This makes cybersecurity measures easier to tailor.

Prevention methods

Regular Security audits

Conducting regular security audits should take place regularly. This also helps with other security preventions such as endpoint security. Endpoint security and security audits should be intertwined to ensure thorough evaluation of endpoints, including updates and assessment of user controls. Endpoint security is crucial for protecting sensitive information and preventing cyber-attacks. Network segmentation is also necessary when

preventing cyber-attacks. This allows the network to split into its own segment which helps gain control over their network by keeping critical systems and sensitive data protected.

Network Monitoring

There is no set duration of network monitoring in correctional facilities as monitoring can vary due to size of the correctional facility, available resources, and appropriate staffing. To protect correctional facilities from inmate information leaks, and vulnerabilities network systems should be monitored 24 hours a day. Specifically human monitoring should be 24hrs to catch any errors in the system that software systems might miss. Automated incident response monitoring could be a useful tool in all correctional facilities. Automated incident response monitoring can "quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents." (Cynet,2024) This would be useful because the system automatically sends an alert when the system is suspected of being under attack.

New detection systems

As the digital age evolves so should detection systems. Deception technology is an effective way to deceive hackers and detect cyber-attacks. This means incorporating fake endpoints, and fake decoy would help trap hackers. Deception technology should also send an alert to staff the moment a hacker is detected.

Employee Training

California prisons went under a cyber-attack from 2020- 2022, this attack “potentially affects 236,000 people” (McGee & Ross, 2022). The problem with this attack is that the staff discovered suspicious activity in January of 2021 and the investigation did not reveal the attack until later that June. This shows that staff were not swift in terms of finding the hacker due to the amount of information that was hacked and how long it took for them to discover this breach. This example shows that educating staff and proper training is important so that attacks do not prolong. Staff should have regular training sessions at least once a month so that cyber protocols are fresh and consistent in their mind. Staff should be able to identify and report any suspicious activity immediately. Staff should also be attentive to spear phishing ensuring they do not click on a spear phishing email or link.

Conclusion

With the progression of the digital age, we see a rapid digital transformation within correctional facilities. As correctional facilities have been evolving over the years new implications such as artificial intelligence, firewalls, and facial recognition are being used to withhold information. New advances in correctional facilities create new challenges that make inmate information, and legal documents harder to protect, along with detecting insider threats. This is why implementing network segmentation, deception technology, and reliable monitoring systems in correctional facilities are essential in providing stable

cyber preventions. Although systems are consistently developed so should staff, staff should be properly educated, trained, and prepared for any cyber-attack that arises.

Works cited

Admin. (2024, January 18). *Prison locks: The evolution and security of the locks*. Bruny Island. https://www.bruny-island.org/prison-locks-the-evolution-and-security-of-the-locks/

American Correctional Association . (n.d.). Staff recruitment and retention in corrections. https://www.aca.org/common/Uploaded files/Publications_Carla/Docs/Corrections Today/2023 Articles/Corrections_Today_Jan-Feb_2023_Staff Recruitment and Retention in Corrections.pdf

Cynet. (2024, January 2). *What is incident response?* https://www.cynet.com/incident-response/

Gillis, A. S. (2022, June 28). *What is a security audit? - definition from TechTarget*. CIO. https://www.techtarget.com/searchcio/definition/security-audit

Puolakka , P., & Steene , S. V. D. (n.d.). Artificial Intelligence in prisons in 2030. https://rm.coe.int/ai-in-prisons-2030-acjournal/1680a40b83

Schappert, S. (n.d.). US prison allegedly hit by Ransomware attack. https://cybernews.com/news/us-prison-play-ransomware-attack-wyatt-detention

Security Technologies for Correctional Facilities. Oosto. (2023, March 10). https://oosto.com/industry/correctional-facilities/

Staff, S. (2018, February 16). *How updated video surveillance maintains safety in correctional facilities*. Security Sales & Integration. https://www.securitysales.com/news/how_updated_video_surveillance_maintains_safety_in_correctional_facilities/

Wasson, M. (2023, November 22). *Enhancing department of corrections investigative units with AI-powered OSINT*. Corrections1. https://www.corrections1.com/enhancing-department-of-corrections-investigative-units-with-ai-powered-osint#:~:text=By%20enhancing%20the%20efficiency%20and,%2C%20inmate%2C%20and%20staff%20safety.