CYBERSECURITY

&

CORRECTIONAL INSTITUTIONS

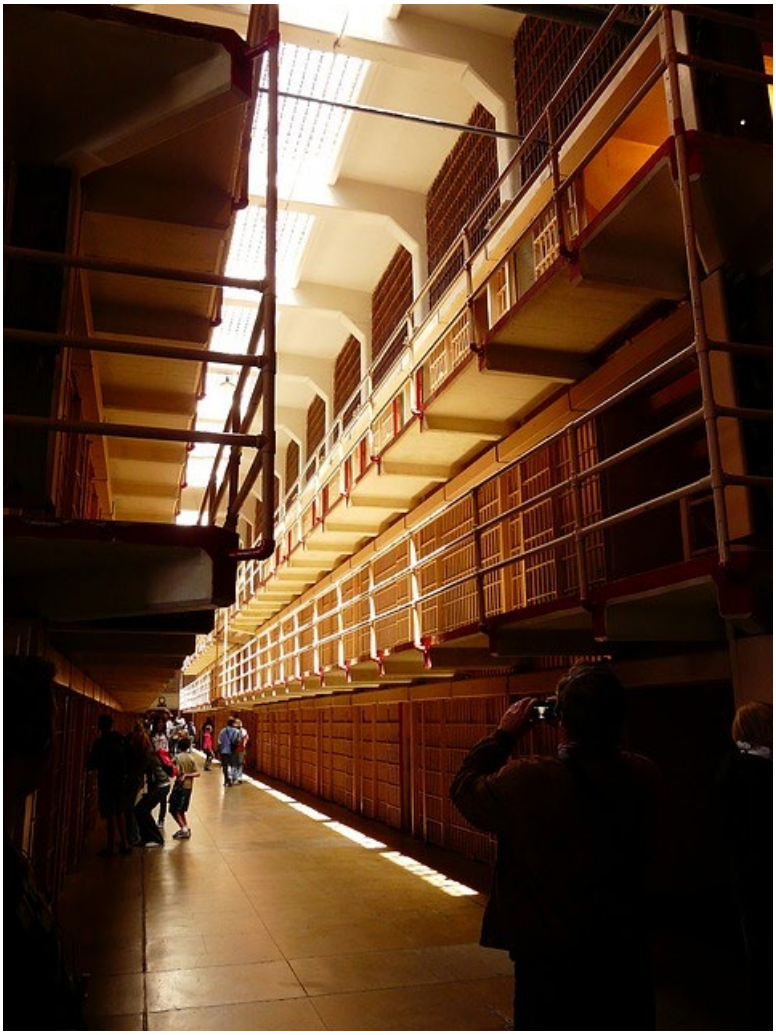
BY:

Kelly Himelwright

Old Dominion University

1. Introduction

Cybersecurity is becoming an increasingly important aspect of correctional operations. To properly maintain security, more jails and prisons are using comprehensive cyber protection techniques. Correctional facilities face risks that were perhaps unimaginable only a few decades ago. Many organizations have used information technology to help them run their businesses, but few have the resources or vision to foresee and adequately manage the cyber dangers that come with it. Institutions need to be more aware of these hazards, as well as have more information security experts on staff. Furthermore, because allowing convicts access to technology to prepare them for reintegration is becoming increasingly vital, it is critical that institutions understand best practices for controlling cyber hazards. We will dive into how essential cybersecurity is for jails and prisons and what the consequence is for not implementing a plan to combat breaches.



Technology advances at a quicker rate than corrections and/or society can keep up. Implementing technology or measures to combat it (for example, cell phones) may be a lengthy and complicated process, and things may have changed by the time new technology is deployed. This package page covers information on computers and the internet, applications, body cameras, biometrics and face recognition, mobile phones, drones, electronic monitoring

and GPS, and x-rays and scanners, in order to give knowledge on the most recent technological advancements in the corrections sector.

2. Background

In prisons, cybersecurity entails monitoring the availability and health status of security devices 24 hours a day, seven days a week. Hackers could take advantage of the vulnerabilities and flaws in the jails' physical security equipment and networks to launch cyber-attacks with potentially disastrous consequences, such as shutting down the video surveillance system. Allowing restricted access to numerous areas, monitoring perimeter crossings, recognizing intrusions as potential breaches, filtering out false alarms, and so on are all part of ensuring the security of prisons and jails. It also entails maintaining close networks with high performance and point security devices that are constantly manned to assure the security equipment's health.

The convergence of physical and cyber security in prisons is increasing and adapting in today's networked reality to incorporate more and more linked gadgets. As they have an impact of the guard operations, video surveillance, and other security systems, designing and implementing efficient cyber defense measures is becoming increasingly important in jails and correctional facilities. While physical security in correctional facilities is obviously important, cyber security is posing new risks in jails and detention centers. Inmates can now exchange messages, read e-books, listen to music, have visitation, and receive money transfers thanks to advances in technology. What happens if a prisoner or a hacker gains access to that technology?

Risk has the same effect on a jail as it does on other organizations: it reduces or improves the jail's capacity to accomplish its objective. Our jail system's objective is to protect the public and maintain a safe environment within the institution in accordance with legal standards, as well as to give job and other self-improvement opportunities to prevent recidivism. Risk management that is done correctly may have a beneficial impact. The importance of cybersecurity and risk management in the penal system will be discussed in this article.

3. Research Gap in Cybersecurity Issues of Correctional Facilities

Security procedures take time and effort to implement, and they typically slow down operations. Employees sometimes disregard fundamental security procedures in order to meet the demands of some jail stakeholders. This might include things like propping a security movement

door open or neglecting to properly identify someone before granting entry to a restricted location. These well-intentioned efforts jeopardize the safety and security of the facility. "The road to Hell is paved with good intentions," as the proverb goes. The term "minimum" is commonly used to denote state prison regulations. They try to develop methods and conditions that will be acceptable to the courts and that indicate fundamental suitable levels based on expert judgment.

Despite the fact that correctional facilities are increasingly embracing technology, they are failing to appropriately manage cybersecurity threats to their systems, assets, and data. The creation and sharing of best practices and lessons learned based on the specific needs of prisons would be beneficial to the sector. Integration of different IP-based technologies into operations should be prioritized, but the institution's network and sensitive data should be protected.

Some dangers to correctional facilities security are as ancient as the facilities themselves, including as violence, escape attempts, and contraband, while others, such as computer hacking, synthetic narcotics, mobile phones, and drones, have developed with social and technical advancements. Many of these issues pose a threat to everyone's safety. RAND researchers conducted an expert workshop to better understand the problems and identify the high-priority needs associated with threats to institutional security in light of the continued issues the correctional sector has in fighting these threats.

3.1 Human Factors

Participants in the expert workshop identified eleven high-priority requirements for preventing threats to institutional security. They are understaffed; staffing ratio guidelines, as well as recruiting and retention tactics, are required to satisfy these standards. In order to effectively develop employees, supervisors need greater training and a controllable span of authority. To identify employees who are prone to compromise, tools are required. To identify narcotics, mobile phones, and weapons, better technology and best practices are required. To prevent the influx of narcotics and safeguard employees and convicts from damage, fully electronic mail systems should be investigated. To assess developing technology solutions to risks, research and testing labs are required (e.g., cell phones, drones). Administrators need to be more aware of cyber threats and IT-related issues, as well as have more ability to deal with them. To combine convict access to technology for reintegration with security issues, best practices are

required. For security threat group management, best practices are essential. In order to analyze prisoner conversations automatically, technology is required. To establish continuity of operations strategies, best practices are required.

Correctional organizations in numerous states are now suffering from chronic and severe understaffing. According to sources referenced in the RAND analysis, officer vacancy rates in certain states are as high as 45%. Annual prison and jail turnover in the United Jurisdictions averages 20%, with some states seeing as much as 53%. "Inadequate personnel impedes an institution's capacity to deter, prevent, and respond to security risks," the research said (RAND, 2022).

A shortage of resources for state correctional agencies is aggravated by a lack of national staffing standards that agencies require to make a persuasive argument to legislators for further funding. As a result, the working group requested that research be conducted in order to produce models that indicate the best staffing numbers. The essential interplay between correctional supervisors and officers, which informs institutional culture and has an influence on security, is a focus of attention for the working group in the area of personnel. Supervisors are frequently hampered in their ability to work efficiently because they are required to fill in for missing officers and are stretched too thin in their supervision of police, compromising their efficiency. The working group emphasized the need for enhanced supervisory training in order to engage employees, as well as study into the short- and long-term consequences of supervisor shortages.

3.2 Raising Issues with New Technology

What makes cybersecurity different from other organizations is that technology advances at a quicker rate than corrections and/or society can keep up. Implementing technology or measures to combat it (for example, cell phones) may be a lengthy and complicated process, and things may have changed by the time new technology is deployed. This package page covers information on computers and the internet, applications, body cameras, biometrics and face recognition, mobile phones, drones, electronic monitoring and GPS, and x-rays and scanners, in order to give knowledge on the most recent technological advancements in the corrections sector.

Let’s look at an example; the 2018 JPay incident if you’re having problems comprehending cybersecurity in correctional facilities. JPay, which bills itself as “you home for

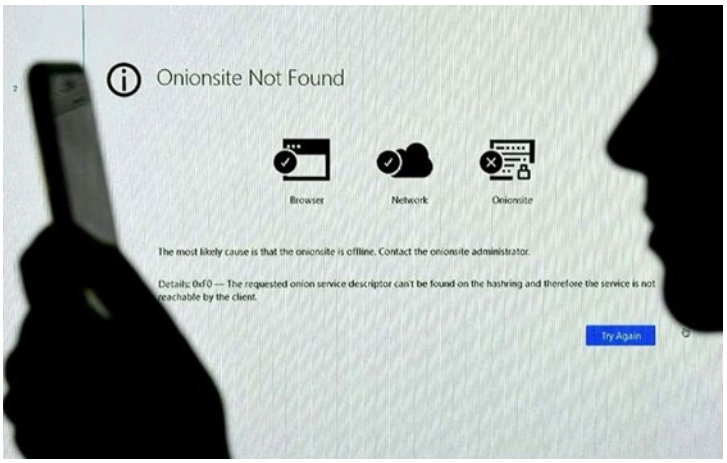
corrections services," is a service provider that focuses solely on correctional facilities (Wired, 2018). JPay isn't the only company that provides services to correctional facilities, but it is one of the most extensively used. In 20 states, it is the sole provider of e-messaging services. It had provided tablets specifically designed for inmates, along with e-messaging and other services.

Hundreds of Idaho inmates, however, discovered a means to credit their JPay accounts with thousands of dollars in 2018. According to the Idaho Department of Corrections, over 300 inmates in five correctional facilities knowingly credited their JPay accounts by $224,772.40, which "required a knowledge of the JPay system and multiple actions by every inmate who exploited the system's vulnerability to improperly credit their account." Fortunately, neither taxpayer funds nor inmates' bank accounts were impacted by this occurrence; only their JPay accounts were affected. However, this incident demonstrates a lack of awareness of cybersecurity for correctional facilities, as well as the fact that new technology has weaknesses that must be addressed.

Data has been compromised by Securus Technologies, a jail technology business that provides phone and video visiting services. An unnamed hacker obtained 70 million records of phone calls made by convicts in at least 37 states in 2015, along with links to digital recordings. When you consider the nature of the calls, this is terrible enough for Securus. At least 14,000 of the recorded talks were between inmates and their attorneys, calls that should have never been captured in the first place under the law to safeguard attorney-client communications. "This may be the greatest widespread breach of the attorney-client privilege in modern history," according to David Fathi, head of the ACLU's National Prison Project, according to the Intercept (ACLU, 2018). Because of their conviction and detention, many of a prisoner's rights are restricted, but the attorney-client privilege does not. In addition to the 2015 breach, Securus was claimed to have sold law enforcement data in 2018 that allowed them to search up the position of cell phones on all the major U.S. mobile networks.

3.3 Ransomware Attacks

Following a ransomware assault on January 5, 2022, an Albuquerque jail lost access to its video feeds and its automatic door mechanisms were rendered inoperable. As a result, inmates have been confined to their cells as technicians work to restore service. Visitor access to the Metropolitan Detention Center was fully halted while the facility was placed on lockdown, as first reported by Source New Mexico. All internet services at the jail were also shut off, making it impossible for personnel to check up inmate data.



3.4 Inmates with Technical Background

Another tale out of Ohio had five offenders who created a pair of functional PCs out of e-waste parts as part of a program aimed to teach computer skills by having inmates break down end-of-life machines and recycle the parts. The convicts snuck the computers into a training room, concealed them in the ceiling, and routed cabling to link to the prison network. The huge win came when the prisoner IT operations team connected the devices to the network of the Ohio Department of Rehabilitation and Correction. They went straight to the races after that. Inmates allegedly peeked over a jail employee's shoulder to acquire his password. They sought to exploit the devices for a variety of cybercrimes once they were in the system, including stealing the identity of another convict serving a long term and applying for many credit and debit cards in

his name. One of the detainees even utilized the laptops to text his mother, informing her where she could get the illegally obtained cards!

When a device "exceeded a daily internet use threshold," the method was found by the rectification networks support staff. The login belonged to an employee who wasn't scheduled to work on those days. However, while the finding was made in July 2015, the incident is only now becoming public, generating considerable concern in the Ohio prison community.

3.5 DDoS Attack

APT-69420, a Swiss-based hacker activism group, infiltrated Verkada security cameras in jails and prisons in March 2021, in order to demonstrate the vulnerability of security cameras. Cyber threat actors hired by organized crime drug traffickers to deliver illegal substances hacked the Belgian port of Antwerp in October 2013. Other cyber threat actors might use the Antwerp assault technique to permit the passage of contraband in and out of prison institutions, as they did with port security cameras. There is a genuine danger. It affects judicial institutions in terms of finances, human health and safety, and day-to-day operations

A hacker might overload the electrical system that controls prison doors by obtaining control of a jail's industrial control system (ICS). Hackers might also disable a jail's communications systems and disable closed-circuit television monitors, leaving prison guards in the dark.

According to the United States Computer Emergency Readiness Team, a distributed denial-of-service (DDoS) assault delivers multiple spam requests to a network, overloading it to the point of a sluggish crawl or a total stoppage (US-CERT). Legitimate users are unable to access a website or websites as a result. DDoS attacks are not unheard of in correctional

facilities. A large DDoS assault targeted twenty Thai jails in January 2016. These hacks can be carried out by anybody, although the hacktivist organization Anonymous is the most prevalent perpetrator. Network security is always in jeopardy, and administrators must ensure that their data is safeguarded.

An expert panel discovered that when correctional institutions' commitment to IT systems grows, so does their commitment to cybersecurity. Security systems, HVAC, communications, health and safety platforms, and other vital correctional activities rely on IT, which is frequently delivered or managed, or both, by outside suppliers. Large, susceptible data collections are frequently kept by agencies. Breach of security is becoming more prevalent. The NIJ-sponsored working group recommended developing best practices for addressing vulnerabilities as well as recommendations for monitoring threats posed by jailed people using Wi-Fi operating networks in close vicinity to institutions to address cybersecurity issues.

4. Current Solutions

What are the options for dealing with this situation? In a perfect world, you'd have a comprehensive cybersecurity program in place, with personnel assigned defined tasks and duties for keeping your critical infrastructure secure. However, there are a few things that may be done to lessen the likelihood of a facility being hacked. Defense-in-depth techniques, such as a mix of physical security and cybersecurity investments, effective network maintenance, investment in cybersecurity training for workers and leadership, and the establishment of a long-term cybersecurity culture, are all part of the final plan.

For correctional institution door control systems, Programmable Logic Controllers (PLCs) are utilized as a standard. Because PLC systems lack virus protection and operate on an open platform, they are particularly vulnerable to cyber-attack. In order to keep PLC systems safe against intrusion, more caution must be used. In order to ensure system security, these systems must be air-gapped or kept behind a highly secure firewall. To prevent infiltration through an ethernet connection, interfaces to video systems and systems that link to external networks should be connected via serial connections. To keep infections out of the system, USB flash drive ports must be turned off. To keep dangers at bay, the Human Machine Interface (HMI) system requires the removal of access to a keyboard and windows.

Nelysis has created a one-of-a-kind system called Vanguard that is designed to fulfill both cyber and physical security concerns in jails and correctional facilities. The NCM solution from Nelysis visualizes the networks and their various elements to detect a wide range of suspicious activities and cyber-threats; Vanguard then notifies the PSIM/command of any changes or network intrusions in order to automatically mitigate their efforts and ensure the prison's operations' continuity and security.

By integrating physical and cyber security in prisons, Vanguard is able to eliminate human error while also providing a redundant approach to overall security. This patent-based system, which was developed expressly for early detection, warning, and prevention of cyber threats on physical security elements and control system networks, enabled for the monitoring of all security network vulnerabilities and health status.

Vanguard is particularly well-suited to the security of jails and penal facilities, which is one of the advantages of employing it for continuous cybersecurity in prisons. Vanguard constantly monitors the physical security devices and control network that are vulnerable to the failure of crucial systems, the neutralization of edge devices, and the disruption of operations caused by a hostile takeover or internal actions such as a faulty setup or even a guard's mistake. Vanguard examines the network's structure identifying and following all network elements. Manufacturer data, network metrics, and physical/logical topology are used to identify network elements. Any unauthorized physical monitoring of infrastructure connections, any damage or connection to optical fibers or copper cables are all examples of such changes.

Vanguard is capable to preventing hostile actors from infiltrating an existing network, searching for and obtaining critical data before an attack on any major network component takes place. It is simple to install and operate, and unlike other IT network security solutions, it does not require any high-level network or cyber-network understanding. Lastly, it has built-in and post-event analysis features, as well as real-time monitoring, control, and robust defense.

5. Conclusion

The commitment of correctional facilities to information technology (IT) systems is growing, but their commitment to cybersecurity is not keeping pace. Security systems, HVAC, communications, health and safety platforms, and other vital correctional functions rely on IT, which is either delivered or managed, or both, by outside suppliers. Large and fragile data collections are frequently maintained by agencies. Breach of security is becoming more regular. The NIJ-sponsored working group recommended developing best practices for addressing vulnerabilities and recommendations for monitoring threats posed by jailed people using Wi-Fi operating networks in close proximity to institutions to address cybersecurity issues.

Unfortunately, funding and personnel constraints restrict correctional facilities' capacity to respond to threats and update security and staffing measures over time as threats change. Furthermore, efforts to create effective treatments to mitigate risks are hampered by a constant shortage of empirical evidence. One way to provide correctional institutions with the assistance they need to face security risks in the future is to address research requirements and develop tools and resources.

Institutional security risks might be as ancient as the institutions themselves. Other risks have arisen in response to cultural and technical advances (e.g., computer hacking, synthetic medicines, mobile phones, and drones). Many of these hazards pose a threat not just to the institution, but also to the general public's safety. Unfortunately, budget and personnel constraints limit correctional facilities' capacity to alter security and staffing measures in response to changing threats. Furthermore, efforts to create effective treatments to mitigate risks are hampered by a constant shortage of empirical evidence. One way to provide correctional institutions with the assistance they need to face security risks in the future is to address research requirements and develop tools and resources, as highlighted by workshop participants.

What can be done to protect prisons against cyber-attacks? In a perfect world, you'd have a comprehensive cybersecurity program in place, with personnel assigned defined tasks and duties for keeping the critical infrastructure secure. However, there are a few things that may be done to lessen the likelihood of a facility being hacked. To provide better mitigation, the ultimate plan employs defense-in-depth. A mix of physical security and cybersecurity investments, effective network maintenance, investment in cybersecurity training for workers

and leaders, and the establishment of a long-term cybersecurity culture are some of the approaches that could be used.

In order to prevent cybersecurity risks, I believe that correctional facilities should have a risk assessment policy. A few additional things to consider include improved technology and best practices for detecting drugs, mobile phones, and weapons, as well as entirely electronic mail systems to limit drug influx and safeguard employees and inmates. To assess new technology solutions to risks, research and testing labs are required (e.g., cell phones, drones). Administrators need to be more aware of cyber threats and IT-related issues, as well as have more ability to deal with them. To combine convict access to technology for reintegration with security issues, best practices are required. For security threat group management, best practices are essential.

For daily cell administration, release date calculation, and other purposes, correctional facilities are progressively using automation and IT technologies. There is evidence that this growing use is creating new vulnerabilities. The easiest method to overcome this stumbling block is to create best practices that are suited to correctional agencies' specific vulnerabilities (and data management needs). Wireless internet access networks near universities are frequently utilized for communication, and they might be difficult to spot. Create a plan for keeping an eye on the threat. Newer infrastructure management equipment (HVAC, steam plants, water systems, and so on) are frequently constructed with connection, which raises vulnerabilities (i.e., the internet of things). Investigate best practices for managing these devices.

References:

Experts identify priority needs for addressing correctional agency security threats. (2020, April 6). National Institute of Justice. https://nij.ojp.gov/topics/articles/experts-identify-priority-needs-addressing-correctional-agency-security-threats

Faife, C. (2022, January 11). A ransomware attack took a New Mexico jail offline, leaving inmates in lockdown. The Verge. Retrieved March 22, 2022, from https://www.theverge.com/2022/1/11/22878471/ransomware-attack-new-mexico-jail-lockdown-cameras-bernalillo-county

Harvey, S. (2020, February 27). Secure your city: Cybersecurity for correctional facilities: Kirkpatrickprice. KirkpatrickPrice Home. Retrieved March 22, 2022, from https://kirkpatrickprice.com/blog/secure-city-correctional-facilities/

Martin, M. D., & Reiss, C. L. (2008, April). Managing Risks in Jails. Cloud Object Storage – Amazon S3 – Amazon Web Services. https://s3.amazonaws.com/static.nicic.gov/Library/022666.pdf

Paul, T. W. B. F., & Paul, F. (2017, April 17). Cybercrime-from inside an Ohio prison. Network World. Retrieved March 22, 2022, from https://www.networkworld.com/article/3190273/cybercrimefrom-inside-an-ohio-prison.html

Russo, J., Woods, D., Shaffer, J. S., & Jackson, B. A. (n.d.). Countering threats to correctional ... - rand corporation. Countering Threats to Correctional Institution Security. Retrieved March 22, 2022, from https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2933/RAND_RR2933.pdf

Zercoe, C. (2016, December 9). DDoS cyberattacks: 3 things correctional administrators should know. Corrections1. Retrieved March 22, 2022, from https://www.corrections1.com/corrections-training/articles/ddos-cyberattacks-3-things-correctional-administrators-should-know-gzXn7mqeFu7D5EDS/