International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 04 Issue 10 October 2021

DOI: 10.47191/ijsshr/v4-i10-03, Impact factor-5.586

Page No: 2642-2649

The Curious Case of the $8 Million Carnegie Library Heist

Donald L. Buresh, Ph.D., J.D., LL.M.
Morgan State University

ABSTRACT: This paper discusses and analyzes the Carnegie Library heist by Greg Priore, assisted by John Schulman, the owner of Caliban Book Shop. The essay outlines the sequence of events that led up to the arrest and conviction of these two individuals. The article then reviews the lists of insider threat indicators that several authors have proposed. Third, the insider threat indicators that would have identified Greg Priore were highlighted. Best practices to recognize an insider threat actor are described. Finally, the article concludes by stating potential lessons learned and observing that focusing on security is a dynamic process where constant vigilance is essential.

KEYWORDS: Caliban Book Shop, Carnegie Library of Pittsburgh, Greg Priore, Insider Theft Actors, John Schulman

INTRODUCTION

There is an adage that is particularly relevant here. It says, "Keep your friends close, but keep your enemies closer."[1] An enemy or a friend is sometimes open to debate, particularly when friends can become enemies and enemies can become friends. In this instance, a friend and a seemingly loyal employee of the Carnegie Library of Pittsburgh, Greg Priore, chose to betray the trust that had been given to him. Over 25 years, Priore sold precious items from the Oliver Room for money. His apparent reasons for his theft were financial. Priore needed to pay his rent and the tuition that ensured that his four children attended private schools. It was a sad affair that should never have happened, where the greatest tragedy was his betrayal of his employer for personal gain.

The paper first discusses the $8 million heist, chronologically outlining what occurred. Second, various lists from several experts of insider indicators are described. Third, the paper examines what insider indicators would have identified Greg Priore before he wreaked havoc on the library's ancient collection of books and documents. Fourth, the essay highlights insider threat best practices. Fifth, the different actions that the Carnegie Library could have done either prevent the heist from occurring in the first place, or minimizing the extent of the theft, recognizing that it may have taken some time to identify the loss of invaluable books and documents. Finally, the essay concludes by highlighting the lessons learned and observing that it is not always possible to prevent insider threat actors from betraying their duty of loyalty. Even so, steps can and should be taken to minimize and alleviate an organization's potential and actual losses.

THE $8 MILLION CARNEGIE LIBRARY HEIST

The $8 million Carnegie Library heist of rare books and documents[2] is an interesting case because it demonstrated that insider threat actors exist in the rarefied atmosphere of information technology and the mundane world of stuffy libraries. For decades, the Oliver Room in the Carnegie Library of Pittsburgh housed a virtual cornucopia of rare books and documents, and the manager of this fortress of ancient knowledge was Greg Priore, an individual who oversaw the entry into the Oliver Room by employees, patrons, scholars, and sometimes curiosity seekers, and a master of science in library science from Pittsburgh University.[3] The room possessed a single entrance and exit. Anyone wanting to review the treasured documents had to leave their items, such as jackets and backpacks, in a locker outside of the room.[4] Priore sat at a desk that permitted him to see the table where the entrants worked

[1] SUN TZU (TRANSLATED BY RALPH D. SAWYER), THE ART OF WAR (Barnes & Noble Books 1994). What this adage means is that one should know one's enemies much better than what one knows one's friends.
[2] Travis McDade, *The Inside Story of the $8 Million Heist from the Carnegie Library*, THE SMITHSONIAN (Sep. 2020), available at https://www.smithsonianmag.com/arts-culture/theft-carnegie-library-books-maps-artworks-180975506/.
[3] Id.
[4] Id.

and labored in gathering the knowledge from these ancient tombs.[5] It was almost as if Priore was the warden in Jeremy Bentham's *Panopticon* prison, wherefrom any angle, the warden of the prison could see the inmates' cells.[6]

In Spring 2017, the Carnegie Library discovered that many of the Oliver Room's books and documents were missing.[7] According to Epstein, books such as the Journal of George Washington, Isaac Newton's *Philosophiae Naturalis Principia Mathematic*a (valued at $1 million), the *Theatrum Orbus Terrarum*, also known as the *Blaeu Atlas*, created by a German explorer of the 19th Century (worth $1.2 million), and other books and documents had just disappeared.[8] [9] After an independent audit was completed, it was estimated that $8 million of rare books and documents had vanished.

Travis observed that two kinds of people frequently visited special collections that were available for public inspection.[10] Some scholars desired to study a particular subject or individuals who just wanted to satisfy their curiosity.[11] Both groups of people were attracted to incunables, or book, pamphlet, or broadside that was printed in Europe before the year 1500.[12] These are documents that were printed using moveable type between 1450 CE and 1500.[13] Incunables are old, rare, and essential when attempting to understand what happened during the Renaissance.[14] [15] The *Blaeu Atlas* was crucial because it contained 276 hand-colored lithographs that mapped the known world when it was written.[16] All 276 lithographs were missing. The copy that the Carnegie Library owned was printed in 1644.[17]

Most of the Carnegie Library's holdings were donated by Andrew Carnegie, the library's founder, along with his friends. In one instance, the library purchased 40 volumes of photogravure prints of Native Americans created by Edward Curtis in the early 20th Century. There were 272 sets created, and in 2012, Christie's sold one set for $2.8 million.[18] The Carnegie Library owned approximately 1,500 photogravure illustrations that were produced by Curtis that were not included in the 40 volumes.[19] Except for a few prints, the vast majority of the photogravure prints were removed from their binding.

Priore worked for the Carnegie Library from 1992 to 2017, or about 25 years.[20] He stole a first edition of the *Wealth of Nations* by Adam Smith, a letter written by William Jennings Bryan, a rare copy of Elizabeth Cady Stanton's 1898 memoir, *Eighty Years and More: Reminiscences 1815-1897*, the first edition of a book written by President John Adams, the second president of the United States, and a book signed by Thomas Jefferson, the writer of the Declaration of Independence and the third president of the United States.[21] Priore absconded with the first English edition of Giovanni Boccaccio's Decameron that was printed in London in 1620, the first edition of George Elliot's *Silas Marner*, also published in London in 1841, and 108 of the 155 hand-colored lithographs from John James Audubon's *Quadrupedes of North America* that was written between 1851 and 1854.[22] Essentially, Priore took any document of any value in the 25 years he worked at the Carnegie Library.

According to Travis, Priore was an easygoing individual that knew a great deal but "wore his knowledge lightly" and lived within walking distance of the prestigious library.[23] When Priore was first hired, he worked with a perseveration specialist who assessed the library's rare and antiquarian books and documents. At the time, it was discovered that the metal shelves leached acid into the books, and so the library established climate controls and upgraded the security system. In 2016, the library officials determined that it was time to audit their collection again and hired the Pall Mall Art Appraiser to perform the appraisal. Kerry-Lee Jeffrey and Christiana Scavuzzo began the audit on April 3, 2017. Within an hour of starting the audit, they could not find Thomas

---

[5] Id.
[6] GILLIAN DARLEY, FACTORY (Reaktion Books, Ltd. 2003), *available at* https://archive.org/details/factoryobjekt00darl/mode/2up.
[7] McDade, *supra*, note XXX.
[8] Kayla Epstein, *Archivist and bookseller plead guilty to pilfering $8M in rare texts from Carnegie Library*, THE WASHINGTON POST (Jan. 4, 2020), *available at* https://www.washingtonpost.com/history/2020/01/14/carnegie-library-book-theft/.
[9] Travis, *supra*, note XXX.
[10] Id.
[11] Id.
[12] *Incunables*, THE FREE DICTIONARY (n.d.), available at https://www.thefreedictionary.com/incunables
[13] Travis, *supra*, note XXX.
[14] Id.
[15] History.com Editors, *Renaissance*, HISTORY.COM (last updated Aug. 27, 2021), *available at* https://www.history.com/topics/renaissance/renaissance.
[16] Travis, *supra*, note XXX.
[17] Id.
[18] Id.
[19] Id.
[20] Epstein, *supra*, note XXX.
[21] Travis, *supra*, note XXX.
[22] Id.
[23] Id.

McKenney and James Hall's *History of the Indian Tribes of North America*. This work included 120 hand-colored lithographs. They found the three-volume set hidden on the top shelf at the end of a row, where most of the plates had been carved out and gone.[24]

The appraisers found that many of the priceless books and documents with illustrations had been looted. Everywhere the appraisers looked, they found destruction and pillaging. On April 7, 2017, after only five days of auditing, Jeffrey and Scavuzzo met with Mary Frances Cooper, the director of the library, and explained to Cooper what was discovered. On April 11, 2017, had the lock to the Oliver Room was changed, and Priore was not given a key.[25]

According to Travis, the only thing that restrains an insider from stealing is a conscience.[26] Physical security measures may frustrate an outside thief, but if a steward wants to steal something, there is little that an organization can do to stop them. In this instance, Priore took the *crème de la crème* from the Oliver Room.[27] Priore and his family lived modestly, but his children attended private schools. According to Travis, Priore committed the crimes to remain solvent.[28] He was not only four months behind in his rent payments but also was attempting to juggle tuition payments for his four children.

Because Priore could walk to work in fifteen minutes, his route took him past the Caliban Bookstore owned and operated by John Schulman, a reputable individual in the antiquarian community. Schulman treated the documents that he purchased from Priore like any of the other rare and old good, but for the material obtained from Priore, Schulman placed a bright red stamp on the bottom of the bookplate, saying, "Withdrawn from Library, thereby allowing him to sell the merchandise without destroying its value"[29] Thus, given Schulman's reputation, his actions ensured that he was the ideal fence for Priore.[30]

When the audit began, Priore readily knew that he would be caught six months before the audit occurred. Priore talked to Schulman about the audit, and the bookseller sent Priore several emails, outline various explanations that Priore could use to explain the missing books and documents. In Fall 2016, when the library administrators debated whether to conduct an appraisal of the Oliver Room's contents, Priore was against the audit.[31] When the auditor discovered the missing documents, Priore argued that the previous director sold off some of the collection when Priore was on leave at Schulman's suggestion. Following Schulman's advice, Priore also contended that the Oliver Room security system was porous, accessible, and imperfect. On April 18, 2017, Priore acknowledged that he often left catalogers, interns, and volunteers alone in the room. Finally, Priore noted that maintenance workers that had worked on the roof also had access to the Oliver Room.[32] The Pittsburgh police started a formal investigation in June 2017, and on August 24, 2017, officers executed a search warrant of Priore's apartment, the Caliban Book Shop, and the Caliban warehouse.[33] When law enforcement executed the search warrant of the Caliban warehouse, they asked Scavuzzo to accompany them. Together, they discovered numerous stolen antiquarian items that belonged to the library. After charging Priore and Schulman with theft and receiving stolen goods, and Schulman with forgery, in July 2018,[34] law enforcement contacted dozens of private collectors, librarians, and rare book collectors to find out what they purchased from Schulman. The result was that Carnegie Library was able to recover many of its precious books and documents.[35]

On January 13, 2020, Priore and Schulman pled guilty to theft and receiving stolen property, while Schulman also pled guilty to forgery.[36] After the audit, the Pall Mall Art Advisors found that over 300 items valued at approximately $8 million had been stolen between 1992 and 2017.[37] In the end, Priore admitted that greed motivated him to steal the antiquarian items, and Schulman had encouraged him to continue the heist.

LIST OF INSIDER THREAT INDICATORS

There are a variety of insider threat indicators. Dosal observed that there are eight insider threat indicators.[38] First, a malicious insider may begin to attempt systems or data that they would not normally access. Second, a future insider threat actor may attempt to discover ways and means to access sensitive information before starting an attack. Third, an insider may transfer computer files

[24] Id.
[25] Id.
[26] Id.
[27] Id.
[28] Id.
[29] Id.
[30] Id.
[31] Id.
[32] Id.
[33] Id.
[34] Epstein, *supra*, note XXX.
[35] Travis, *supra*, note XXX.
[36] Epstein, *supra*, note XXX.
[37] Id.
[38] Eric Dosal, *8 Insider Threat Indicators to Watch out For*, COMPUQUIP (Mar. 30, 2020), *available at* https://www.compuquip.com/blog/insider-threat-indicators.

to hard copy to have no computer record of an attack.[39] Fourth, an insider threat actor may regularly send and receive emails to and from individuals outside the organization who are not clients, vendors, or business partners. Fifth, a would-be attacker may attempt to access data after work or when on vacation.[40] Sixth, individuals plotting an insider attack may suddenly change their behavior towards their coworkers by becoming short-tempered or dismissive, or possibly suddenly ecstatic or sociable.

Seventh, the attacker may attain sudden financial wealth without explaining where they received the fortune. Finally, after carrying out an attack, many insiders decide to quit their positions as a means of covering their tracks.[41]

According to Zhang, there are several early indicators of an insider threat happening.[42] Poor performance appraisals, voicing disagreement with policies, disputes with coworkers, financial distress, unexplained financial gain, odd working hours, unusual overseas travel, or quitting their position may all point to the existence of an insider threat.[43] Help Systems Staff stated five suspicious signs of a malicious insider threat, comprising unusual logins, the use or recurrent attempted use of unauthorized applications or data, a significant increase in access privileges, excessive use or downloading of data, or unusual employee behavior when compared the behavior of other employees.[44]

Rosenthal listed eleven factors that could signify that an insider threat actor existed with an organization.[45] Declining job performance or other signs of dissatisfaction, unusual or long working hours, large data transfers or downloads, multiple logins that fail or other abnormal login activity, privileges that are upgrade or sharing access with other people, or unexpected changes in financial circumstances may specify that an insider threat actor is present.[46] Additional indicators include consistent, and possibly unusual, overseas travel, a failure to comply with basic or corporate security policies, a low or an overly high engagement or appreciation of security policies, a history of succumbing to phishing attacks, or a general sense of careless or haste, or possibly an overly intense sense of security.[47]

Finally, according to the Defense Security Service, a single indicator is insufficient to determine whether an insider threat actor exists.[48] Potential espionage indicators include repeated security violations with a general indifference of security rules, failure to report overseas travel or contact with foreign nationals when the security rules demand disclosure, seeking higher or desiring to expand access outside the scope of the job without a need to know, having classified conversations without a need to know, physically entering or attempting to enter areas without authorization, working long hours that is not authorized by the job description, or accessing or attempting to access information beyond the scope of the position.[49] Behavioral traits that an insider threat actor may express are depression, the stress in one's personal life, use of drugs, alcohol, gambling, financial trouble, or previous disciplinary issues.[50] Other suspicious behaviors involved are a sudden reversal of an individual's financial position, being disgruntled coupled with the desire to retaliate, reoccurring or unnecessary work outside of regular business hours, bringing an unauthorized electronic, such as a cell phone, into a secured area, or threatening the safety of people or property.[51]

As one can readily observe, there are seemingly many signs or indicators that point to an insider threat actor existing within an organization. As previously stated, there is no one determining characteristic of an insider threat actor. It is only by examining that a significant set of indicators that one can possibly conclude that the existence of an insider threat actor is appropriate.

INSIDER INDICATORS THAT WOULD HAVE IDENTIFIED GREG PRIORE

Hindsight is always 20/20. In this case, various indicators could have identified Priore as an insider threat actor, provided that someone in authority above Priore had noticed. One of the key indicators that could point to an insider threat actor is that Priore worked for the Carnegie Library for 25 years.[52] The senior directors at the library could have believed that Priore was not a threat

[39] Id.
[40] Id.
[41] Id.
[42] Ellen Zhang, *The Early Indicators of an Insider Threat*, DIGITAL GUARDIAN (Aug. 11, 2020), *available at* https://digitalguardian.com/blog/early-indicators-insider-threat.
[43] Id.
[44] Help Systems Staff, *Five Malicious Insider Threat Indicators and How to Mitigate the Risk*, CORE SECURITY (n.d.), *available at* https://www.coresecurity.com/blog/five-malicious-insider-threat-indicators-and-how-mitigate-risk.
[45] Maddie Rosenthal, *Insider Threat Indicators: 11 Ways to Recognize an Insider Threat*, TESSIAN (Jun. 17, 2020), *available at* https://www.tessian.com/blog/insider-threat-indicators-how-to-recognize-an-insider-threat/.
[46] Id.
[47] Id.
[48] Defense Security Service, *Insider Threat*, COUNTERINTELLIGENCE DIRECTORATE (n.d.), *available at* https://home.army.mil/bragg/application/files/3215/0515/6485/InsiderThreat.pdf.
[49] Id.
[50] Id.
[51] Id.
[52] Travis, *supra*, note XXX.

because of the length of time that he worked for the organization. Second, a possible sign that Priore was a potential insider threat was he was an easygoing individual who "wore his knowledge lightly."[53] This could have been a market that Priore did not take the security of the Oliver Room seriously. Third, Priore lived within walking distance of the library, possibly suggesting that if he wanted to work long hours or enter the library at odd hours, it would have been relatively easy for him to do so.[54]

When Priore was hired, he worked with the preservative specialist that the library had employed to preserve its collection.[55] Priore was probably aware that the metal shelves used at the time leaked acid into the antiquarian books and documents. Also, when the Oliver Room security system was installed in the 1990s, Priore was in an excellent position to learn the quirks of the security system thoroughly when it was installed, particularly its climate controls. There was one entrance into the Oliver Room, and the position of Priore's desk permitted him to watch all of the patrons to the room as they studied the texts.[56] When an individual left the room, Priore checked that the book or document was intact.[57] Over time, this fact gave Priore intimate knowledge of the contents of the Oliver Room, particularly those items that were of significant value.

Priore lived modestly, but his children went to private schools. Based on Priore's job description, it is unlikely that he made sufficient income to afford to send his four children to private schools. Although the library staff probably ignored it, Priore may have complained to his associates about his children's high cost to ensure that they received a private education. This was likely a clear indicator that Priore was living beyond his means, notably when Travis wrote that Priore was juggling tuition payments.[58] Although this indicator would have been hard to spot, simply because Priore may not have discussed his financial situation with his peers, the fact he was four months behind in his rent payments pointed to the possibility that Priore was the individual who was responsible for the heist.[59] He needed money to remain solvent.

When the library wanted to audit and appraise their collection in 2017, Priore argued against it.[60] This behavior could be construed to be unusual because the last audit was conducted 25 years ago. Based on the time between audits, it seems more than reasonable that the library management would want to perform another appraisal to discover the current value of its collection.[61] Priore also argued that the previous director who was dead had sold several books and papers in the collection.[62] However, not in and of itself a vital indicator of an insider threat, together with the fact that Priore argued against the appraisal, it could prompt one to ask if Priore was hiding something. Priore's admission that the security system was imperfect could have raised some concerns with the library's senior directors.[63] After all, Priore was a library employee when the security system was installed.[64] If anyone had known how to make the security system more perfect or knew all of the system flaws, it would be Priore.

When inserting Schulman into the equation, the isolation of an additional indicator gets harder. One critical indicator is the time that Priore spent at the Caliban Book Shop.[65] Because Priore walked to work, and because the Caliban Book Shop was on his way to work, on the days that Priore visited the bookshop before he came to work, it was likely that he may have arrived late to the Carnegie Library. Priore may have been conversing with Schulman on many subjects, thereby increasing his time to go to work or his time to arrive home. On the days that Priore visited Schulman, his potential tardiness could indicate that Priore was an insider threat actor. As for Schulman, if Priore was alone when he met Schulman, the meeting itself may not have been seen as a potential threat.

Schulman's emails to Priore regarding what to say in case Priore was caught might have been an indicator if Priore had employed a Carnegie Library email address.[66] If Priore only communicated with Schulman via email through his personal email account, the library management would not necessarily have known of the interactions. It should be remembered that the library did not have the right to invade Priore's emails from his private account without Priore's expressed written consent. Thus, provided that Priore used a personal email account, there may have been no probable cause, let alone reasonable suspicion, for the library to investigate Priore's emails. If Priore had accessed his private email account while using the library's servers, then there was the possibility that a sufficiently sophisticated Internet application could have captured Priore's emails to Schulman. There was no indication that the security system included such erudite software.

---

[53] Id.
[54] Id.
[55] Id.
[56] Id.
[57] Id.
[58] Id.
[59] Id.
[60] Id.
[61] Id.
[62] Id.
[63] Id.
[64] Id.
[65] Id.
[66] Id.

INSIDER THREAT PREVENTION BEST PRACTICES

Although many authors that address best practices for preventing insider threats deal with computer access issues, many of the specified best practices carry over to this case. According to the Netwrix Staff, a variety of best practices can be employed to prevent insider threats from occurring.[67] First, an organization should conduct perform periodic enterprise-wide risk assessments. This means that an enterprise-wide risk assessment should be accomplished at pre-specified intervals. Second, an entity should clearly and expressly document and consistently enforce existing policies and controls. In other words, the policies and rules in place should be easy to understand and unfailing implemented. Third, the physical security of the work environment in the work environment should be instituted and followed, where few, if any, exceptions are allowed. Fourth, the organization should implement security software and appliances so that violations of security policies and controls are flagged and monitored by individuals charged to administer security.[68]

Fifth, strict password and account management policies and practices should be consistently applied when software security is at issue. Sixth, an organization should monitor and control both physical and remote access, particularly mobile devices. Seventh, harden the physical and network perimeter security. In other words, it should be made difficult to enter or exit a secured area.[69] Eighth, enable surveillance and periodically review the surveillance recordings of the activities of individuals both inside the perimeter of the secured site and when they enter and exit the protected area. Ninth, enforce the separation of duties and least privilege by requiring that two individuals execute security policies and controls.[70] This tenet makes it harder for a single individual to become an insider threat actor because it would take the consent of a second individual to instigate a security threat. Tenth, identify individuals who could violate the organization's policies and controls and respond promptly to suspicious behavior. Eleventh, develop a comprehensive employee termination procedure so that employees understand and appreciate the consequences of violating the organization's security policies and controls. Twelfth, as part of an employee training program, the entity should develop insider threat awareness training and require employees to participate in security training at least once a year.[71] The remaining best-practice items highlighted by the Netwrix Staff deal exclusively with software security and do not seem to apply in this instance.

Kohen highlighted five best practices that bear explaining.[72] First, train employees in data management, or in this case, ancient book and document management, best practices. Second, establish, communicate, and enforce content management standards. This best practice turns out to be crucial in this instance. Third, protect the perimeter by monitoring it both physically and electronically. Fourth, anticipate privilege misuse by both users and individuals charged with enforcing security policies and procedures. Finally, develop a proactive approach to security to become an integral part of an employee's daily routine.[73]

According to the National Insider Threat Task Force (NITTF), nine best practices can be implemented to neutralize insider threat actors.[74] First, decide who should be responsible for supervising all aspects of the insider threat issue. Second, identify the "crown jewels," or those that could detrimentally affect the organization if stolen or destroyed, including tangible and intangible products, formulas, production techniques, software, algorithms, and customer information. Third, periodically and timely reassess security management procedures. Fourth, develop clear termination procedures so that would-be insider threat actors unambiguously understand the consequences of violating security policies and controls.[75]

Fifth, engage the workforce in security so that potential insider threat actors become well aware that their peers are watching them. Sixth, periodically review physical and software systems for security violations and vulnerabilities. Seventh, hire third-party security experts to evaluate the security policies and procedures periodically within an organization. Eighth, put insider threat information into the appropriate context to understand what constitutes normal and abnormal behavior. And finally, regular tests of the security policies and controls should be put in place to identify any vulnerabilities.[76] If a vulnerability is discovered, modify the security policies and rules accordingly.

---

[67] Netwrix Staff, *Insider Threat Prevention Best Practices*, NETWRIX (n.d.), *available at* https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html.
[68] Id.
[69] Id.
[70] Id.
[71] Id.
[72] Isaac Kohen, *Insider Threat Prevention: 5 Steps to Improving Defensive Posture By the End of 2021*, BUSINESS 2 COMMUNITY (Aug. 10, 2021), *available at* https://www.business2community.com/cybersecurity/insider-threat-prevention-5-steps-to-improving-defensive-posture-by-the-end-of-2021-02424521.
[73] Id.
[74] NITTF Staff, *Protect Your Organization from the Inside Out: Government Best Practices*, NATIONAL INSIDER THREAT TASK FORCE (2016), *available at* https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf.
[75] Id.
[76] Id.

DIFFERENT ACTIONS AND LESSONS LEARNED

The Carnegie Library could have prevented or mitigated the theft by following the best practices discussed above. First, create a security director or manager position, and fill the position with an individual who is not one of the people assigned to monitor the daily activities in the Oliver Room. This action would dramatically reduce the risk of having the fox protect the hen house. Second, assign two people to watch the Oliver Room patrons. The advantage of having two people in the room rather than just one person is that the two individuals would not only be observing the activities of the Oliver Room patrons, but they would also be watching each other. Third, document security policies and controls and then enforce them religiously, where no one can violate the guidelines without good cause. Fourth, cameras should be placed everywhere and recorded, and there should be no blind spots. The Carnegie Library should hire a third party to investigate and ensure no blind spots are present within the Oliver Room. Fifth, the surveillance recordings should be reviewed by an individual who reports to a director of the Carnegie Library and not one of the two people charged with monitoring the activities within the Oliver Room. Sixth, identify any employee who could likely be an insider threat actor based on the individual's position within the Carnegie Library. Also, identify any library employee that exhibits several of the traits of an insider threat actor, and for these individuals, closely monitor their activities. Seventh, train all Carnegie Library employees to be security conscious at all times. For the people involved in securing the ancient books and documents within the Oliver Room, additional training should be provided to ensure that they possess a heightened awareness of security. The training would probably instill in these people the idea that they would be quickly caught if they attempted to steal ancient books and documents. The training would likely act as an effective deterrent to potential pilferage. Testing security is critical to discover its vulnerabilities. Management can become complacent without periodically testing a firm's security policies and controls, thereby virtually giving an insider threat actor *carte blanche* to steal corporate assets, significantly disrupting the entity's activities or both. Finally, and probably most importantly, the Carnegie Library should periodically audit the contents of the Oliver Room, say one every two years. The fact that it took 25 years to conduct a second audit of the room's contents is wholly unacceptable. Assuming that Priore stole books and documents of approximately the same total value from year to year, the library would have only experienced a loss of $640,000, not $8 million.[77] It should be noted that a loss of $640,000 of books and documents is a far cry from a loss of $8 million that the library experienced. The idea is that a bi-annual audit would be expensive but would pay for itself if it was discovered that one of the library's employees was illegally procuring and selling library assets, such as the rare books and documents contained in the Oliver Room.

CONCLUSION AND LESSONS LEARNED

The lesson learned from the Carnegie Library heist is that complacency when it comes to security is a risky venture. An organization must be constantly vigilant when it comes to security. Continuous improvement is essential when the risk of loss is substantial. Suppose an organization believes that its security policies and rules are sufficient, and an insider threat actor exploits this situation. In that case, the entity will not only suffer economic losses, but a significant decline in the goodwill of its employees, clients, and patrons, leading to a substantial loss of trust in the community. Reputations are built over time with hard-earned trust but can be lost in an instant if one or more of the members of an organization fail to honor their duty of loyalty or due care to the organization. Even if the Carnegie Library had followed all and more of the recommendations above, there is no guarantee that someone in the future would pilfer their collection of antiquarian collection of rare books and documents. As Robert Burns once wrote many years ago, "The best laid schemes o' mice an' men, Gang aft a-gley," or translated, the best-laid plans of mice and men can still go wrong.[78] In other words, no matter how well one plans, there is never a guarantee of success. Security is no exception to this rule.

REFERENCES

1) SUN TZU (TRANSLATED BY RALPH D. SAWYER), THE ART OF WAR (Barnes & Noble Books 1994). What this adage means is that one should know one's enemies much better than what one knows one's friends.
2) Travis McDade, *The Inside Story of the $8 Million Heist from the Carnegie Library*, THE SMITHSONIAN (Sep. 2020), available at https://www.smithsonianmag.com/arts-culture/theft-carnegie-library-books-maps-artworks-180975506/.
3) GILLIAN DARLEY, FACTORY (Reaktion Books, Ltd. 2003), *available at* https://archive.org/details/factoryobjekt00darl/mode/2up.
4) McDade, *supra*, note XXX.

[77] The average yearly value of goods stolen by Priore was $320,000 (= $ 8 million / 25 years). If an audit had been conducted every two years, the approximate amount that Priore may have stolen would be $640,000 (= 2 years * $320,000 of goods stolen per year).

[78] Robert Burns, *To a Mouse*, POETRY FOUNDATION (n.d.), *available at* https://www.poetryfoundation.org/poems/43816/to-a-mouse-56d222ab36e33.

5) Kayla Epstein, *Archivist and bookseller plead guilty to pilfering $8M in rare texts from Carnegie Library*, THE WASHINGTON POST (Jan. 4, 2020), *available at* https://www.washingtonpost.com/history/2020/01/14/carnegie-library-book-theft/.
6) Travis, *supra*, note XXX.
7) *Incunables*, THE FREE DICTIONARY (n.d.), available at https://www.thefreedictionary.com/incunables
8) Travis, *supra*, note XXX.
9) History.com Editors, *Renaissance*, HISTORY.COM (last updated Aug. 27, 2021), *available at* https://www.history.com/topics/renaissance/renaissance.
10) Travis, *supra*, note XXX.
11) Epstein, *supra*, note XXX.
12) Travis, *supra*, note XXX.
13) Epstein, *supra*, note XXX.
14) Travis, *supra*, note XXX.
15) Epstein, *supra*, note XXX.
16) Eric Dosal, *8 Insider Threat Indicators to Watch out For*, COMPUQUIP (Mar. 30, 2020), *available at* https://www.compuquip.com/blog/insider-threat-indicators.
17) Ellen Zhang, *The Early Indicators of an Insider Threat*, DIGITAL GUARDIAN (Aug. 11, 2020), *available at* https://digitalguardian.com/blog/early-indicators-insider-threat.
18) Help Systems Staff, *Five Malicious Insider Threat Indicators and How to Mitigate the Risk*, CORE SECURITY (n.d.), *available at* https://www.coresecurity.com/blog/five-malicious-insider-threat-indicators-and-how-mitigate-risk.
19) Maddie Rosenthal, *Insider Threat Indicators: 11 Ways to Recognize an Insider Threat*, TESSIAN (Jun. 17, 2020), *available at* https://www.tessian.com/blog/insider-threat-indicators-how-to-recognize-an-insider-threat/.
20) Defense Security Service, *Insider Threat*, COUNTERINTELLIGENCE DIRECTORATE (n.d.), *available at* https://home.army.mil/bragg/application/files/3215/0515/6485/InsiderThreat.pdf.
21) Travis, *supra*, note XXX.
22) Netwrix Staff, *Insider Threat Prevention Best Practices*, NETWRIX (n.d.), *available at* https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html.
23) Isaac Kohen, *Insider Threat Prevention: 5 Steps to Improving Defensive Posture By the End of 2021*, BUSINESS 2 COMMUNITY (Aug. 10, 2021), *available at* https://www.business2community.com/cybersecurity/insider-threat-prevention-5-steps-to-improving-defensive-posture-by-the-end-of-2021-02424521.
24) NITTF Staff, *Protect Your Organization from the Inside Out: Government Best Practices*, NATIONAL INSIDER THREAT TASK FORCE (2016), *available at* https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf.
25) The average yearly value of goods stolen by Priore was $320,000 (= $ 8 million / 25 years). If an audit had been conducted every two years, the approximate amount that Priore may have stolen would be $640,000 (= 2 years * $320,000 of goods stolen per year).
26) Robert Burns, *To a Mouse*, POETRY FOUNDATION (n.d.), *available at* https://www.poetryfoundation.org/poems/43816/to-a-mouse-56d222ab36e33.