Report for The Seattle Public Library
After-Action Review (AAR)

Adaptable Security Corp

(Doing Business As Cybertrust America)

March 2025

Table of Contents

I. Executive Summary

This report presents the findings of an After-Action Review (AAR) conducted by Cybertrust America ("Cybertrust") to comprehensively assess The Seattle Public Library's (the "Library" or "SPL") response to a ransomware attack discovered on May 25, 2024. (the "Incident").

As an independent nonprofit coalition, Cybertrust was selected from a pool of qualified consulting firms to conduct the AAR. Cybertrust's deep-rooted experience in local government partnerships and proven cybersecurity methodologies enabled the team to assess the incident response, provide expert insights, and recommend practical, collaborative, and cost-effective improvements.

Cybertrust coordinated with SPL's executives, SPL Information Technology ("SPL IT"), the City of Seattle's Information Technology ("City IT"), Seattle City Attorney's Office ("City Attorney"), Seattle City's outside legal counsel ("Legal Counsel") and SPL's incident response vendors, to develop this AAR Report.

The AAR reviewed the entire Incident lifecycle, from initial detection to final recovery. This included initial detection, response initiation, containment, and stakeholder communication. The response showcased many strengths, including but not limited to, rapid activation of the Incident Response Plan, decisive leadership, effective collaboration with internal and external partners, and timely communication with stakeholders.

The AAR also identified opportunities to strengthen SPL's incident response. A pragmatic roadmap is developed to capitalize these opportunities, including:

- **Risk-based Management:** Expanding the use of a risk-based approach will maximize the impact of investments by prioritizing risks and focusing efforts on the most critical areas.
- **Dedicated Cybersecurity Leadership:** Centralized leadership, with a designated cybersecurity leader and team, could improve accountability and foster a stronger cybersecurity posture as compared to a decentralized approach.
- **Cybersecurity Culture with Partners:** By leveraging SPL's strong collaborations and partnerships with City of Seattle's departments, such as City IT, the City Attorney's Office, and the Mayor's Office, SPL can foster a stronger cybersecurity culture. This can be achieved through formal agreements like Memorandum of Understanding (MOUs), which can unlock valuable resources, expertise, talent, and grant opportunities.

The Seattle Public Library leadership restated its commitment to bolster its cyber defenses and enhance its protection of its 10 million annual patrons, its dedicated workforce, as well as its invaluable 2.9 million items in its collection, ensuring the continued fulfillment of its mission “to bring people and ideas together to enrich lives.”

II. The Cyber Incident and Response

In the early hours of Saturday, May 25, 2024 of Memorial Day weekend, SPL discovered a ransomware attack and took proactive actions to disrupt the threat actors’ advances. The actions included suspending services in its central downtown location, 26 neighborhood branches and two data centers. Buildings remained open at the Library’s 27 locations across Seattle, with print books and other physical materials available for checkout via paper forms while access to staff and public computers, online catalog and loaning systems, e-books and e-audiobooks, in-building Wi-Fi, and the Library website were affected.

Swift actions led to the restoration of key services thanks to the Library’s Incident Response Team, consisting of Library personnel, outside legal counsel, and forensics experts. By May 26 all online machines and servers had security software enabled, and laptops paired with wifi hotspots were available for Library staff to deliver library services. External communications was established on May 28 via the ShelfTalk blog. The external Domain Name System (DNS) was restored on June 4, enabling the www.spl.org public web site to resume online services. All e-materials including e-books and e-audiobooks were restored by June 13, 2024. The Library’s services were fully restored by September 4th. This recovery time of 72 business days ranks in the top 5% for performance, according to the IBM Ponemon Institute's "Cost of a Data Breach Report 2024."

With the assistance of outside experts, the Library undertook an extensive investigation to better understand what occurred during the attack and what data may have been affected. The investigation determined that while it is challenging to pinpoint the threat actor’s unauthorized initial entry into SPL’s systems, the activities were consistent with the compromise of a Virtual Private Network (VPN) appliance. The threat actors used this initial foothold to expand their attack, and beginning on May 24, 2024, the threat actors downloaded SPL data and deployed ransomware on SPL systems. Impact to the Library patrons’ data was minimized thanks to the Library’s policy of storing minimal patrons’ personally identifiable information.

With the assistance of outside experts, the Library undertook a complex and labor-intensive process to identify personal data contained in those files and locate up-to-date contact information for impacted individuals. While this process was underway, the Library took the proactive step of offering credit monitoring services to all employees and setting up call center support. Following the completion of its analysis of the impacted data, SPL promptly gave formal notice to all identified individuals as appropriate beginning on December 12, 2024. The notices included an offer for two years of free credit and identity monitoring services. This AAR applies the latest NIST Cybersecurity Framework 2.0 and the Incident

Response Recommendations and Considerations for Cybersecurity Risk Management, and summarized the following:

Areas of Success:

- **Clear Leadership and Strong Teamwork**: The responsive leadership and collaborative spirit allowed the Library to respond to the Incident swiftly and effectively.
- **Rapid Response and Collaboration**: The Incident Response Plan (IRP) was properly activated and followed once the Seattle Public Library IT lead received the notification of the Incident.
- **Leveraging External Expertise**: Third-party consultants provided critical expertise and resources to accelerate the recovery process.
- **Flexible and Adaptive Approach**: The ability to adapt to changing circumstances and to make timely decisions was crucial, e.g., necessary actions were taken swiftly despite the attack taking place on a holiday weekend and that some leaders were on scheduled vacation.

Lessons Learned:

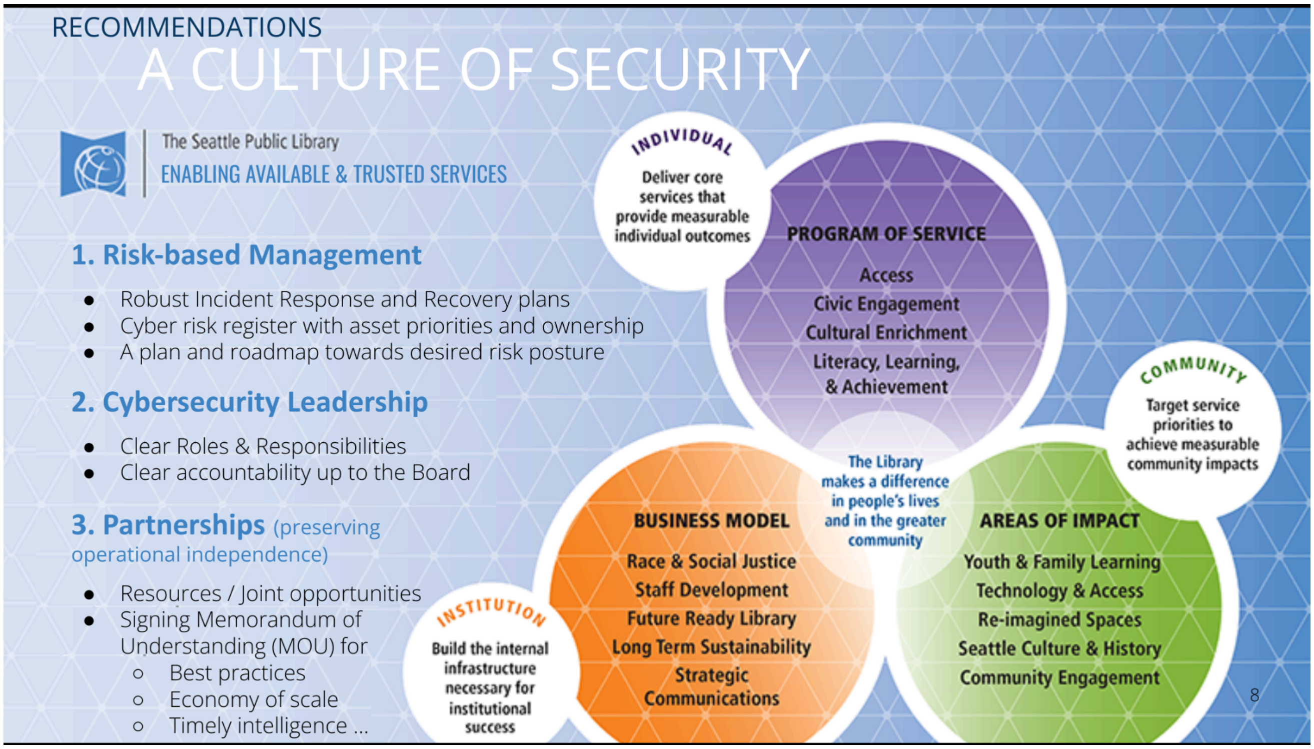
1. Consider standing up a Security Operations Center (SOC) function with clearly defined service agreements and performance metrics.
2. Enhance Incident Response Planning by:
    - Strengthening the communication protocols by establishing out of band communication and logging systems
    - Identifying and tracking incident response performance metrics such as Mean Time to Recover (MTTR)
    - Conducting annual tabletop exercises to practice deploying the Incident Response Plan (IRP) and Continuity of Operations Plan (COOP)

III. Recommendations

It is imperative that the Library continue to safeguard its services and protect all Library and employee data including patrons and employees' data from cybersecurity risks in alignment with SPL's mission and guiding principles: "Protect confidentiality of patron records", "Form strong partnerships," and "Adapt and innovate."

A. Three Opportunities to Enable SPL's Mission

The AAR has identified three opportunities that the Library can leverage to improve its cybersecurity maturity in a cost-effective way over time. Figure 1 below illustrates these opportunities.



RECOMMENDATIONS

A CULTURE OF SECURITY

The Seattle Public Library

ENABLING AVAILABLE & TRUSTED SERVICES

1. Risk-based Management

- Robust Incident Response and Recovery plans
- Cyber risk register with asset priorities and ownership
- A plan and roadmap towards desired risk posture

2. Cybersecurity Leadership

- Clear Roles & Responsibilities
- Clear accountability up to the Board

3. Partnerships (preserving operational independence)

- Resources / Joint opportunities
- Signing Memorandum of Understanding (MOU) for
  - Best practices
  - Economy of scale
  - Timely intelligence ...

INDIVIDUAL
Deliver core services that provide measurable individual outcomes
PROGRAM OF SERVICE
Access
Civic Engagement
Cultural Enrichment
Literacy, Learning, & Achievement
COMMUNITY
Target service priorities to achieve measurable community impacts
The Library makes a difference in people's lives and in the greater community
BUSINESS MODEL
Race & Social Justice
Staff Development
Future Ready Library
Long Term Sustainability
Strategic Communications
AREAS OF IMPACT
Youth & Family Learning
Technology & Access
Re-imagined Spaces
Seattle Culture & History
Community Engagement
INSTITUTION
Build the internal infrastructure necessary for institutional success
8

Figure 1 Recommendations: A Culture of Security Enables SPL's Available and Trusted Services

We recommend that the Library develop a pragmatic roadmap which considers both asset criticality and cybersecurity risks in an effort to capitalize on these three opportunities and submit that developing such a roadmap would assist the Library in realizing its desired cybersecurity maturity on schedule. We propose that the first step the Library takes when designing such a roadmap is to conduct a rigorous risk assessment.

Strengthening the Library's cybersecurity leadership could leverage the NICE Workforce Framework for Cybersecurity (NICE Framework) to staff the Library with qualified personnel.

B. Success Measurements

You can't manage what you don't measure. To effectively enhance SPL's cybersecurity posture and culture, we recommend tracking key metrics, such as:

1. Cybersecurity Posture   This metric is highly confidential on a need-to-know basis, enabling the cybersecurity leader and team's planning and accountable execution.

2. Transparency   Stakeholders understanding SPL’s cybersecurity strategy, knowledge, and commitment cultivates a sense of ownership and responsibility, fostering a robust security culture.
3. Stakeholder Confidence   Stakeholders’ level of confidence in SPL’s ability to protect its assets and personnel can guide the Library’s cybersecurity strategy and plans.

By tracking these metrics annually or semi-annually, the Team can identify trends, measure progress, and make data-driven decisions to accomplish its cybersecurity program goals.

C. AAR Report Verification

The Library has taken steps to address some of the recommendations contained in this AAR. For example, the Library has been establishing a dedicated cybersecurity leadership and has filled the position of a dedicated cybersecurity analyst. A Security Operations Center (SOC) has been acquired to provide more robust monitoring to ensure SPL’s availability.

To maximize the value derived from this After-Action Review (AAR), Cybertrust recommends an AAR Report verification within six months no later than August 1, 2025. This verification will evaluate the progress made in implementing the recommendations in this report. A concise verification report will be appended to this document to capture the findings and any necessary adjustments to the original recommendations.

IV. Conclusion

This AAR concludes that the Library managed the incident response effort effectively and as a result, lessened the impact of the ransomware attack. This outcome is attributed to strong leadership, effective execution of the incident response plan, and strong partnerships that enabled a service restoration timeline which outperformed the global average for data breaches.

The AAR has yielded valuable insights and actionable recommendations for further enhancing the Library's incident response planning. By implementing these recommendations, the Library can continue to strengthen its incident response processes and documentation to ensure even greater efficiency and resilience.

Furthermore, the AAR report outlines a risk-based management methodology and proposes a pragmatic roadmap for achieving a robust cybersecurity posture. Successful implementation of this roadmap will significantly enhance the Library's cyber defense, improving its availability, safety, and overall ability to fulfill its mission for all stakeholders.

Cybertrust is honored to have contributed to this AAR effort and remains committed to supporting SPL and City of Seattle’s cybersecurity initiatives as needed.

Appendices

Appendix A Abbreviations

AAR

An after-action review (AAR) is a technique for improving process and execution by analyzing the intended outcome and actual outcome of an action and identifying practices to sustain, and practices to improve or initiate, and then practicing those changes at the next iteration of the action.

NIST CSF

National Institute of Standards and Technology. It is an agency under the Department of Commerce. CSF refers to the Cybersecurity Framework, which includes 153 controls with 26 new controls in the new pillar “Govern”. https://www.nist.gov/cyberframework

NICE

The NICE Workforce Framework for Cybersecurity (NIST Special Publication 800-181, revision 1) provides a set of building blocks for describing the Tasks, Knowledge, and Skills (TKS) that are needed to perform cybersecurity work by individuals or teams. Through these building blocks, the NICE Framework enables organizations to develop their cybersecurity workforces and helps learners explore cybersecurity work and engage in learning activities to develop their capabilities. https://niccs.cisa.gov/workforce-development/nice-framework

MTTR

Mean time to recovery /respond /resolve /repair (MTTR) is the average amount of time it takes to repair or recover from an issue or failure in a system, equipment or process.

COOP

Continuity of Operations Plan (COOP)

SOP

Standard Operating Procedures

Appendix B References

1. National Institute of Standards and Technology, Cybersecurity Incident, https://csrc.nist.gov/glossary/term/cybersecurity_incident
2. The Seattle Public Library "Strategic Direction" https://www.spl.org/about-us/the-organization/strategic-direction
3. The Seattle Public Library, Shelf Talk Blog, https://shelftalkblog.wordpress.com/2024/05/28/an-update-about-access-to-library-technology-systems/
4. IBM Ponemon Institute, "Cost of a Data Breach 2024," https://www.ibm.com/reports/data-breach
5. Nationwide Cybersecurity Review: 2023 Summary Report https://www.cisecurity.org/insights/white-papers/nationwide-cybersecurity-review-2023-summary-report
6. Learning Lessons From The Cyber-Attack, British Library cyber incident review, MARCH 8, 2024 https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf/
7. NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
8. Gartner-2024-leadership-vision-for-security-and-risk-management.pdf https://www.gartner.com/en/webinar/579686/1300649
9. Gartner-how-to-build-a-robust-defensible-security-program-that-enables-business-growth-and-agility https://www.gartner.com/en/doc/766390-how-to-build-a-robust-defensible-security-program-that-enables-business-growth-and-agility
10. Top 10 Biggest Government Data Breaches, August 22, 2024 https://www.digitalguardian.com/blog/top-10-biggest-government-data-breaches-all-time-us

Disclaimer

Orrick, Herrington & Sutcliffe LLP ("Counsel") engaged Cybertrust America's services on behalf of Counsel's client, The Seattle Public Library, in connection with a privileged investigation. Cybertrust America's services were performed at the direction of Counsel to assist Counsel in providing legal advice to The Seattle Public Library in response to a computer security incident. Cybertrust America is providing no opinion, attestation or other form of assurance and disclaims any contractual or other responsibility to others based on their access to or use of the Deliverable. Accordingly, the information in this Deliverable may not be relied upon by anyone other than Counsel and Seattle Public Library.

The scope of Cybertrust America's work was confined to reviewing the available documents and forensic evidence provided to us, along with interviewing selected relevant Seattle Public Library employees and vendors pertinent to the review. Although Cybertrust America has taken reasonable measures to verify the accuracy of the information given, we have not independently validated all the information.

Throughout the review, we received a substantial volume of documentation. Our review focused only on those documents deemed relevant to our engagement letter. Consequently, we cannot ensure that we have seen all pertinent documents or information that may exist, nor can we comment on their completeness. Any additional documentation or information brought to our attention after the date of this report may necessitate adjustments to our findings.