2024 -2025 Mono County Civil Grand Jury Investigation Report

Mono County Cybersecurity Preparedness

March 1, 2025
V4.0

SUMMARY

The 2024-2025 Mono County Civil Grand Jury conducted an investigation into Mono County's cybersecurity preparedness, focusing on the County's security posture and Payment Card Industry (PCI) compliance. The investigation was prompted by the increasing vulnerability of local government agencies to cyber-attacks as they transition to digital systems. The grand jury's investigation was guided by Mono County's 2019 Information Technology Strategic Plan, which outlined its two-year cybersecurity objectives.

While the County has made good progress in cybersecurity preparedness as outlined in the Strategic Plan, several gaps were identified:

- Staffing Deficiencies: The County has operated without a Chief Information Security Officer (CISO) since June 2021, leaving cybersecurity responsibilities to be absorbed by existing IT staff, and resulting in slowing progress towards objectives outlined in the strategic plan.
- Testing Gaps: The County lacks regular penetration testing and external vulnerability testing, with no sustainable funding in place for periodic testing.
- Backup Vulnerabilities: The absence of immutable backups places the County at high risk for potential ransomware attacks.
- Infrastructure Risks: Unsupported devices remain in the environment, creating significant cybersecurity vulnerabilities due to lack of security patches and updates.
- PCI Compliance Issues: The County appears to be using an incorrect self-assessment questionnaire (SAQ) for PCI compliance attestation, and the IT department is not involved in the compliance process.

Despite these challenges, the investigation noted positive developments, including successful implementation of quarterly cybersecurity training with a greater than 80% compliance rate among County and City employees.

The grand jury made eight recommendations, including:

- Establishing a cooperative process between Finance and IT for completing the annual PCI compliance self-assessment.
- Developing a plan to implement immutable backups for critical data.
- Creating sustainable processes for regular security testing and device updates.
- Assessing staffing needs for cybersecurity initiatives.

- Implementing quarterly cybersecurity training compliance reporting to County executives.

This report requires responses from the Mono County Board of Supervisors regarding findings F2-F7 and recommendations R2-R8 within 90 days, with an invited response from the Director of Information Technology within 60 days.

GLOSSARY

- **Cyber-Attack**: An attempt to damage, disrupt, or gain unauthorized access to computers, networks, or digital systems with malicious intent.
- **Cyber-Security**: The practice of protecting computers, networks, digital systems, and data from unauthorized access, attacks, and damage.
- **Digital Systems**: Electronic devices, networks, and software applications that process, store, or transmit information in electronic form.
- **Immutable backups**: Copies of data that cannot be modified, encrypted, or deleted once they are created.
- **PCI Compliance**: PCI (Payment Card Industry) is a set of security standards designed to ensure all companies that accept, process, store, or transmit credit card information maintain a secure environment.
- **PCI Self-Assessment Questionnaire (SAQ)**: A validation tool used by businesses to self-evaluate their compliance with credit card security requirements.
- **Penetration Testing**: Penetration testing is a simulated cyber-attack on a computer system, network, or application to identify and assess security vulnerabilities.
- **Ransomware:** A type of malicious software designed to block access to critical data until a sum of money is paid.
- **Threat Actor**: An individual, group, organization or government that attempts or executes a cyber-attack.
- **Vulnerability Testing**: Vulnerability testing is the systematic scanning and examination of computer systems, networks, or applications to identify potential security weaknesses and flaws.

BACKGROUND

According to the FBI's Internet Crime Complaint Center (IC3) 2024 Internet Crime Report, ransomware attacks against state and local government entities continue to pose a significant threat, with government services being among the top targeted sectors. Local government agencies have become increasingly vulnerable to cyber-attacks as they continue to transition critical services and sensitive public data to digital systems. Such systems support public safety, tax collection, property records, court documents, and emergency services – making them attractive targets for cyber criminals. Sophisticated cyber criminals specifically target local governments due to their limited cybersecurity resources and the critical nature of their services. Counties that fail to maintain robust cybersecurity preparedness risk not only financial losses but also disruption to essential public services, damage to citizen trust, and potential legal liability for data breaches.

Given the increasing risks of cyber-attack for local government agencies described above, the Mono County Grand Jury conducted an investigation into Mono County's Cyber Security posture and preparedness. The investigation focused on the County's cyber security readiness across a number of areas described in the Discussion section below. Since the County accepts in-person and web-based credit card payments, the investigation also looked into the County's compliance to the Payment Card Industry (PCI) requirements imposed by the major credit card brands.

During the investigation, the Grand Jury learned the County's Information Technology department provides cybersecurity services to all County departments, including the Sheriff's Department and the Town of Mammoth Lakes. Therefore, findings and recommendations included in this report are intended to benefit all three organizations.

METHODOLOGY

The Grand Jury reviewed the following documents and web resources:

- *Mono County IT Cyber Security Incident Procedures documentation,* Various dates
- *Information Technology Strategic Plan,* 2019
- *Mono County Payment Card Industry Policy,* 2020
- *Mono County's Attestation of Compliance Form SAQ-D,* 2024
- *Mono County Information Technology Organization Chart,* 2024
- *Egbedion, Grace. Impact Of Vulnerability Management And Penetration Testing On Security-Informed IT Project Planning And Implementation. Journal of Engineering Science and Technology,* 2024
- *Verizon Data Breach Investigations Report. Verizon Business,* 2023
- *PCI Security Standards Document https://listings.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf*

Interviews

During the investigation, the Grand Jury interviewed 3 employees with Mono County.

DISCUSSION

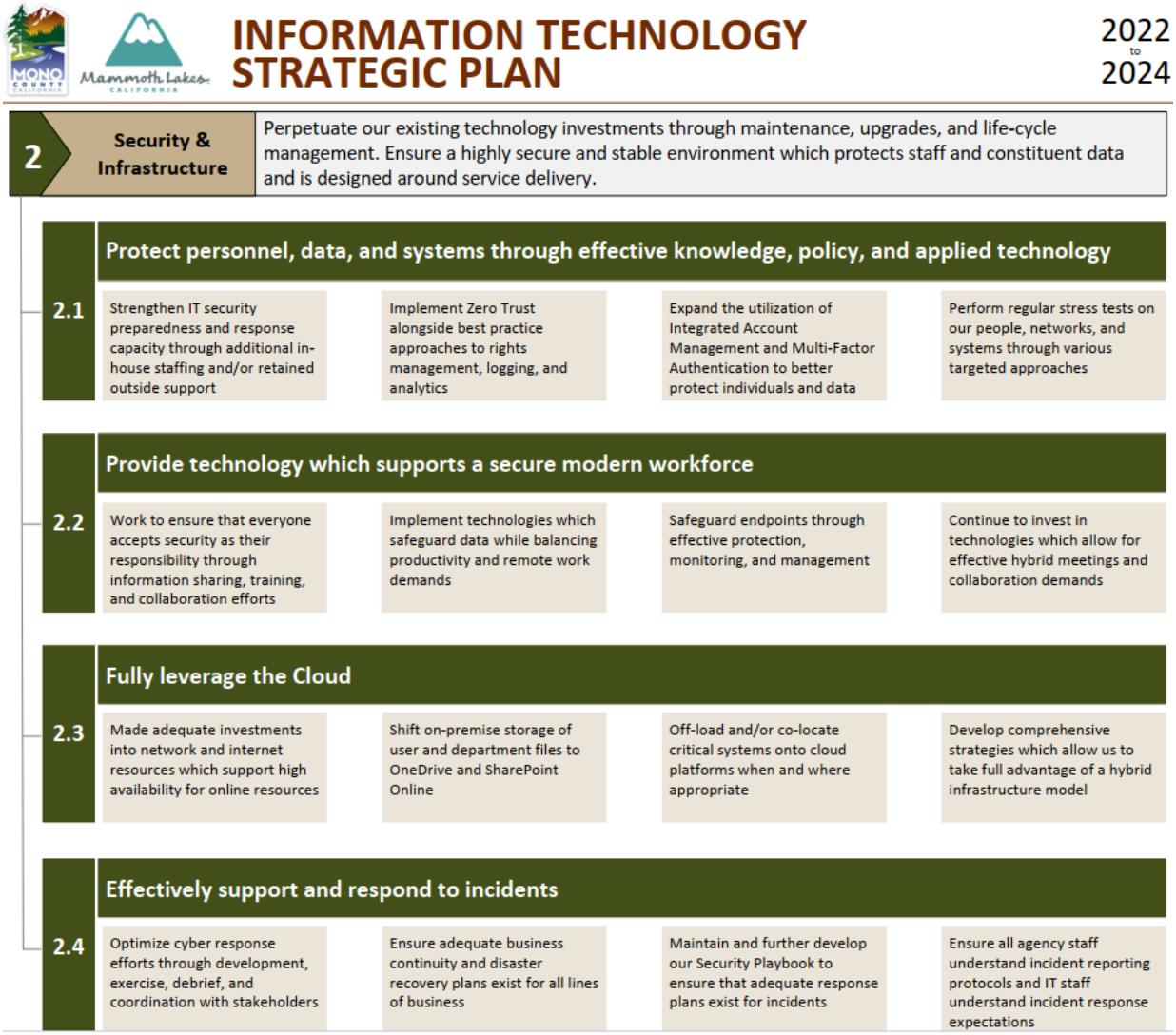
The Grand Jury recognizes cybersecurity is an extremely complicated topic. Specialized knowledge, experience, and expertise are required for a deep understanding of what is necessary to adequately prevent, detect, respond, and recover from a cyber-attack. Therefore, the grand jury's investigation was limited to examining the County's plans to continuously improve its cybersecurity posture, progress against those plans, and compliance to the Payment Card Industry (PCI) requirements.

Guiding the investigation was the County's Information Technology Strategic Plan where cybersecurity objectives and initiatives are documented. The investigation was also guided by publicly available Payment Card Industry (PCI) requirement documents and forms.

Cyber Security Objectives

In 2019, Mono County released a two-year strategic plan that included cybersecurity objectives (Figure 1) to continuously improve the County's security posture.

Figure 1 – Mono County's Information Technology Strategic Plan showing cybersecurity objectives



The Grand Jury was pleased to see cyber security included in Information Technology's strategic plan with clear objectives outlined. Among the strategic plan's four objectives, objective #2 (Figure 1) was most relevant to the Grand Jury's investigation, with sections 2.1, 2.2, and 2.4 of most interest.

Mono County has made good progress towards their cybersecurity preparedness with meaningful accomplishments and completion of most documented initiatives. However, more work is needed to complete all initiatives and continue to mature Mono County's cybersecurity preparedness. A discussion of Grand Jury observations and comments on remaining work is below.

Objective 2.1 - Protect Personnel, data, and systems through effective knowledge, policy, and applied technology.

Objective 2.1 outlines the need for staffing to "Strengthen IT security preparedness". However, the County's IT team lost their part-time Chief Information Security Officer (CISO) in June 2021 and had not filled the position at the time of our investigation. The grand jury understands the

position was the only in-house dedicated staff working on completing cyber security initiatives. As a result of the ongoing vacancy, the remaining IT staff has and continues to absorb the additional cyber security workload. The lack of dedicated staffing to continue progress was cited as a major contributor to incomplete work.

Objective 2.1 also describes the need for "regular stress tests". Vulnerability and penetration testing are key in bolstering cybersecurity resilience and reducing the risks posed by cyber threats (Egbedion, 2024). In addition, PCI Compliance requires quarterly vulnerability scans[1]. The grand jury found regular penetration testing and external vulnerability testing had not been performed, nor was there any funding in place to implement sustained periodic testing. At the time of our investigation, grant funding was being pursued to pay for periodic testing. However, interviewees acknowledged grant funding is unreliable and therefore not an ideal funding source for continuous testing needs.

Objective 2.2 - Provide technology that supports a secure modern workforce.

Quarterly Cyber Security training for employees was in place and compliance was being actively monitored as required by Objective 2.2. Understanding that seventy four percent (74%) of all cyber security incidents include the human element via social engineering or stolen credentials (Verizon, 2023), raising awareness of employees through cyber security training can be an effective strategy. The grand jury learned more than 80% of County and City employees completed their quarterly cybersecurity training videos in 2024 - a noteworthy achievement. However, training compliance measurements are not widely published to County executives which would give visibility to trends and aid continuous improvement.

Of most concern regarding incomplete work under objective 2.2 was the lack of immutable backups. Immutable backups are crucial for ransomware recovery because attackers cannot encrypt or destroy them, ensuring organizations always have access to clean, uncompromised data that can be used to restore systems without paying a ransom. The lack of immutable backups for operational critical data places the County at high risk due to its limited ability to recover from a ransomware attack.

The grand jury also discovered the County's ability to safeguard devices (e.g. PC's, network switches) is at risk due to the fact that vendor unsupported devices are in the environment. Using devices that are no longer supported by vendors creates significant cybersecurity vulnerabilities since such systems no longer receive critical security patches and software updates to protect against newly discovered threats. When vendors end support for computing devices, they stop developing fixes for security flaws, leaving these systems permanently vulnerable to exploitation by threat actors who search for and target such outdated equipment. The lack of funding was cited as a main reason for not replacing unsupported devices in the environment. At the time of our investigation, grant funding was being pursued to pay for replacing unsupported devices. Again, interviewees acknowledged grant funding is unreliable and therefore not an ideal funding source for continually keeping the environment up to date.

Objective 2.4 - Effectively support and respond to incidents.

[1] **PCI Requirements Document v4: Requirement 11.3.2** External vulnerability scans are performed as follows: At least once every three months.

The County has good documentation for procedures to respond to a cyber security incident. However, the grand jury did notice many of the documents appear old with revision dates from over 8 years ago, or are out of date as they list contact information for employees no longer with Mono County.

Objective 2.4 also outlined the need for business continuity and disaster recovery plans. The grand jury learned such plans exist, but the validation of those plans through periodic exercises - such as desktop exercises - are not being performed. Disaster recovery desktop exercises are simulated crisis scenarios where an organization's key personnel gather to verbally work through their response to potential disasters, such as cyber-attacks, natural disasters, or system failures. These exercises are valuable because they allow teams to identify gaps in recovery plans, clarify roles and responsibilities, and practice decision-making in a low-stress environment before a real crisis occurs. The lack of dedicated cyber security staff was cited as a major contributor to not performing disaster recovery desktop exercises.

Payment Card Industry Requirements

PCI (Payment Card Industry) requirements are designed to protect credit card data during and after financial transactions. Organizations – such as Mono County - handling credit card information must comply with PCI requirements which are focused on protecting cardholder data and regularly monitoring and testing systems for vulnerabilities. There are currently 9 different self-assessment questionnaires' (SAQ's) used by organizations to assess their compliance to PCI requirements. How an organization accepts and processes credit card transactions determines which SAQ is used to assess compliance.

The grand jury learned the County has outsourced their credit card processing to a 3rd party vendor, and uses payment terminals to encrypt in-person payments. The grand jury also learned the County's Finance department completes the SAQ each year and attests to the major credit card brands that they meet all PCI requirements. However, there are two issues the grand jury uncovered with the annual completion of the SAQ:

1. **The County appears to be using the wrong SAQ form given they use devices that encrypt credit card payments and process transactions through a 3rd party.** According to the County's last attestation using form SAQ-D, they indicated credit card data is present in their computing environment. However, the County does not store credit card data in the computing environment according to those we interviewed. Selecting the wrong SAQ form can result in failing to implement the required security controls for the County's environment, leaving cardholder data vulnerable to theft or compromise. Additionally, claiming compliance using an incorrect SAQ could be considered misrepresentation, potentially leading to increased liability in the event of a breach and possible fines or penalties from payment card brands.
2. **The County's Information Technology department was not aware of PCI Compliance requirements and the annual SAQ process.** The Information Technology (IT) department has detailed knowledge of the County's technical environment essential for accurately completing an SAQ. Without IT's involvement, the County risks overlooking security controls and misunderstanding their credit card environment, which may lead to inaccurately claiming compliance. For example, the County claimed full PCI compliance in their September 2024 attestation even though PCI requirement 11.3.2 calling for quarterly

vulnerability scans are not being performed. Such inaccuracies should be caught with IT involvement.

FINDINGS

F1. The County regards Cyber Security preparedness as a high priority by taking positive actions to continuously improve its maturity posture resulting in a lower risk of cyber security incidents.

F2. The Payment Card Industry (PCI) self-assessment questionnaire (SAQ) process inadequately involves IT resulting in a lack of IT awareness of the PCI Compliance process and errors on attestation reporting.

F3. The lack of immutable backups results in increased risk of disruption to important County operations due to a ransomware attack.

F4. Computing devices, no longer supported by the vendor, are present in the environment resulting in an increased risk of cybersecurity vulnerabilities and attacks.

F5. The lack of consistent periodic external penetration testing and vulnerability scans results in unknown potential exploits which increases the risk of cybersecurity incidents.

F6. Important Cyber Security projects and initiatives have not begun or are lagging due to insufficient staffing.

F7. Quarterly cyber security training is taking place with noteworthy results. However, there's a lack of visibility to compliance measurements among County executives.

RECOMMENDATIONS

R1. The Grand Jury commends the Information Technology department for their ongoing efforts on cybersecurity preparedness.

R2. The grand jury recommends the Board of Supervisors instruct the Director of Finance and Director of IT to document and put into practice a cooperative process for completing the annual PCI Compliance assessment. Recommendation to be completed by 08/01/2025.

R3. The grand jury recommends the Board of Supervisors instruct the Director of Finance and Director of IT to determine the correct PCI SAQ form(s) to be used in the County's next annual PCI Compliance assessment and attestation. Recommendation to be completed by 08/01/2025.

R4. The grand jury recommends the Board of Supervisors instruct the Director of IT to document a plan to implement immutable backups for operationally critical data. Plan to be documented by 9/01/2025.

R5. The grand jury recommends the Board of Supervisors instruct the Director of IT to define a sustainable annual process to remove or replace unsupported computing devices from the environment. Recommendation to be completed by 08/01/2025.

R6. The grand jury recommends the Board of Supervisors instruct the Director of IT to define a sustainable process to conduct periodic external penetration tests and vulnerability scans. Recommendation to be completed by 09/01/2025.

R7. The grand jury recommends the Board of Supervisors instruct the Director of IT to assess the staffing and capacity demands needed to reasonably support Information Technology's Cyber Security roadmap for the purpose of submitting such staffing in its next fiscal year budget. Recommendation to be completed by 10/01/2025.

R8. The grand jury recommends the Board of Supervisors instruct the Director of IT to implement a process for providing the Board of Supervisors a quarterly report on employee compliance to cybersecurity training. Recommendation to be completed by 10/01/2025.

REQUEST FOR RESPONSES

The following responses are required pursuant to Penal Code sections 933 and 933.05:
From the following governing bodies:

- The Mono County Board of Supervisors: Respond to findings F2 – F7, and recommendations R2 – R8 within 90 days of receipt of this report.

Invited responses

The Grand Jury invites the following individual to respond:

- Mono County Director of Information Technology: Respond to findings F2 – F7, and recommendations R2 – R8 within 60 days of receipt of this report.

Response Submissions

Response must be submitted to the presiding judge of the Mono County Superior Court in accordance with the provisions of Penal Code section 933.05. Responses must include the information required by section 933.05.

Responses can be sent via email to: GJ@mono.courts.ca.gov or mailed to the following address:

Honorable Mark Magit, Presiding Judge
Mono County Superior Court
P.O. Box 1037
Mammoth Lakes, California 93546

Also, please email a copy of the response to Nancy Licari, Staff Secretary to the Grand Jury, at nlicari@mono.courts.ca.gov

Reports issued by the Grand Jury do not identify individuals interviewed. Penal Code section 929 requires that reports of the Grand Jury not contain the name of any person or facts leading to the identity of any person who provides information to the Grand Jury