Cyber Preparedness: Are We There Yet?

May 17, 2024

SUMMARY

Cyber preparedness is the practice of ensuring that an organization has a strategy or plan to prevent, respond to, and recover from a cyberattack or incident. This strategy is a collaborative effort that all of an organization's staff shares in, not just the individuals or department responsible for Information Technology (IT) or Information Systems (IS).

The Grand Jury has looked into how different agencies in Marin County (Marin) have continued to become more cyber prepared in order to meet the ever-changing and more complicated technology challenges required to keep their online content and information secure from hackers and other threat actors. This report also provides an overview of cybersecurity practices and systems currently in existence. This is intended to encourage Marin government entities to review their plans and to consider various options to further enhance their cybersecurity measures.

As a result of its investigation, the Grand Jury is making a number of recommendations including the following four:

1. The Board of Supervisors should authorize the creation of a new position within the Department of Information Services and Technology for the 2025-2026 fiscal year, with specific responsibilities to assist other Marin agencies in cybersecurity awareness, training, implementation and monitoring of cybersecurity systems.

2. Marin agencies should require a current (executed within the last five years), competitively-bid, written contract which includes business continuity language for any third party Information Technology services they use.

3. The Board of Supervisors should require that the Marin Department of Information Services and Technology evaluate the formation of a Cybersecurity Joint Powers Authority to raise overall cyber preparedness among its members, and to acquire and maintain perimeter defense protection systems for preventing and eliminating ransomware and other more sophisticated cyberattacks.

4. The Board of Supervisors should create two new system-engineering positions to be filled by cybersecurity experts who would be responsible for conducting security risk assessments, providing recommendations, and implementing cybersecurity solutions for public agencies in Marin, among their other tasks. If and when a Joint Powers Authority is created, one of these positions would serve as a County member of the new organization and a liaison with the Chief Information Security Officer.

BACKGROUND

In 2020, the Marin County Civil Grand Jury published its report, *Cyberattacks: A Growing Threat to Marin Government*.[1] In the three years leading up to the publishing of the 2020 report, six Marin municipalities had been the target of various cyberattacks.[2] In the 2020 report, the Grand Jury focused its investigation on the security of the computer systems used by Marin's government agencies, and called for increased collaboration and transparency regarding cybersecurity issues affecting government agencies throughout Marin. The report made nine recommendations to these agencies. Below are four of the Recommendations from the 2020 report which the 2023-2024 Grand Jury decided to review. While the 2020 report included nine recommendations, the Grand Jury believed that understanding the progress made with these four would give the best overall indication of Marin's cyber preparedness.

- The County should take a lead role in sharing cybersecurity information and best practices with Marin's cities and towns.
- Cities and towns should implement basic prudent cybersecurity practices, including user training, email filtering, password management, and backups.
- Municipalities should pursue shared cybersecurity services, where feasible, to lower costs and raise their level of security.
- The Marin County Information Services and Technology Department should complete a plan for enhancing the Marin Information and Data Access Systems (MIDAS) to improve cybersecurity for its users.

As a result of the 2019-2020 Grand Jury's first recommendation, the County took the lead in establishing an agency to provide cybersecurity information and best practices to Marin's municipalities. This agency, called the Marin Information Security Collaborative, was initially composed of representatives from the cities and towns of Marin. The agency was later expanded to include other Marin community partners and private organizations, and in 2022 it was renamed Marin Security and Privacy Council (MSPC).[3]

Since the Grand Jury's 2020 report, cyberattacks on a global scale have become more sophisticated, utilizing interactive intrusion techniques, cloud intrusions, mobile device vulnerabilities, and third-party relationship exploitation.[4] The dark web (See Appendix A for a definition) also plays a significant role in cyberattacks due to its anonymity and unregulated nature. It provides a platform for cybercriminals, hackers, and others to operate beyond the reach

[1] Marin County Civil Grand Jury, *2019-2020 Cyberattacks: A Growing Threat to Marin Government,* May 11, 2020, https://www.marincounty.org/-/media/files/departments/gj/reports-responses/2019-20/cyberattacksagrowingthreattomaringovernment.pdf?la=en, (accessed 4/4/24).
[2] Cyberattacks include phishing, ransomware and direct attacks on computer hardware (terms are described in Appendix A).
[3] Digital Marin website, Marin Security and Privacy Council, https://godigitalmarin.org/marin-security-and-privacy-council, (accessed 4/4/24).
[4] Crowdstrike website, *2024 Global Threat Report,* https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf, p. 9, (accessed 4/4/24); Embroker website, *Top 10 Cybersecurity Threats in 2024*, January 4, 2024, https://www.embroker.com/blog/top-cybersecurity-threats, (accessed 4/4/24).

of law enforcement. The dark web is used by cyber criminals to steal information from companies and individuals and sell it.

Due to persistent and increasingly sophisticated malicious cyber campaigns that threatened the public and private sector, and ultimately the American people's security and privacy, President Biden issued Executive Order 14028 in 2021 to improve the nation's cybersecurity.[5] This executive order sought to remove the barriers to threat information sharing between the government and the private sector, improve the security of the software supply chain, and shift the federal government to cloud-based services and Zero Trust Architecture.[6] Many of the key concerns of this executive order were applicable to state, county and local government agencies as well.

Despite Executive Order 14028, cybersecurity attacks have continued to mount, both in frequency and cost to the victims. The *Center for Internet Security's Nationwide Cybersecurity Review* found that cyberattacks on state and local governments increased from 2022 to 2023. The report compared the first eight months of 2022 and 2023, when participating government organizations claimed they saw noticeable growth in several types of cyberattacks. The center found that malware attacks increased by 148 percent, while ransomware incidents were 51 percent more prominent during the first eight months of 2023 than they were during the same period a year earlier.[7]

In a review of IBM's *Cost of a Data Breach Report 2023*, the security awareness company SoSafe reported that the average cost of a cyber incident to an agency in the public sector was over $2.6 million.[8] SoSafe's review also noted that cybercriminals were attracted to public sector websites due to "outdated technology and security measures, limited security budgets and understaffed teams, and the public sector's wealth of sensitive and valuable data." Ransomware attacks against public agencies in the State of California have been well publicized this past year. In some cases, large ransoms have been paid.[9]

---

[5] The White House website, *Executive Order on Improving the Nation's Cybersecurity | The White House*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, (accessed 4/4/24).

[6] See definition of Zero Trust Architecture in Appendix A.

[7] Sophia Fox-Sowell, Cyberattacks on state and local governments rose in 2023, says CIS report, https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024, *StateScoop*, January 30, 2024, (accessed 4/29/24).

[8] SoSafe website, *Top 5 cyber threats facing the public sector*, https://sosafe-awareness.com/blog/top-5-cyber-threats-facing-the-public-sector, (accessed 4/30/24).

[9] Colin Atagi, "St. Helena, Solano County libraries hit by cyberattack, $100,000 ransom demanded", https://www.pressdemocrat.com/article/napa/library-st-helena-solano-cyberattack, *Santa Rosa Press Democrat*, April 22, 2024, (accessed 4/24/24); City of Oakland website, *City of Oakland Restores and Recovers Systems Affected by Ransomware Attack*, April 27, 2023, https://www.oaklandca.gov/news/city-of-oakland-restores-and-recovers-systems-affected-by-ransomware-attack, (accessed 4/4/24); Brian Rokos, "San Bernardino County paid $1.1 million ransom to hacker of Sheriff's Department computers", *San Bernadino Sun*, May 4, 2023, https://www.sbsun.com/2023/05/04/san-bernardino-county-paid-1-1-million-ransom-to-hacker-of-sheriffs-department-computers, (accessed 4/4/24); Andre Byik, "City of Hayward detects Cyberattack, takes down website", *The Mercury News*, July 10, 2023, https://www.mercurynews.com/2023/07/10/city-of-hayward-detects-cyberattack-takes-down-website, (accessed 4/4/24).

There are many published articles, studies, and guidelines on how agencies, as well as private institutions and individuals, can help prevent and mitigate the impact of these attacks. These include reports from the Cybersecurity and Infrastructure Security Agency (CISA),[10] the Federal Bureau of Investigation,[11] JP Morgan,[12] and others.

Due to the ongoing and ever-increasing cybersecurity threats to public agencies posed by numerous and sophisticated adversaries utilizing more advanced cyberattack technologies, the Grand Jury decided to investigate the state of cybersecurity at many Marin agencies. The Grand Jury's investigation also serves as a follow-up to the 2019-2020 Grand Jury's report on the threat of cyberattacks to Marin's governments. This investigation was not designed to point out or highlight specific cybersecurity deficiencies at particular agencies. Rather, it was undertaken to see what improvements had been made in their cyber preparedness and to see if other recommendations should be made to further enhance overall cyber preparedness across agencies in Marin County.

APPROACH

In its investigation of cyber preparedness in Marin, the Grand Jury undertook the following actions:

Interviewed:

- Representatives from different County agencies
- Representatives from each of Marin's 11 towns and cities
- Members of water, health, sanitation, and utility districts
- A member of a third-party organization providing IT and cybersecurity services to the County, and to Marin's towns and cities

The Grand Jury also:

- Reviewed articles, surveys, and research papers concerning cybersecurity practices and the use of shared services arrangements in local governmental agencies

The Grand Jury's investigation into cyber preparedness concluded on April 24th, 2024.

Please refer to Appendix A for a list of cybersecurity terms and acronyms.

[10] Cybersecurity & Infrastructure Security Agency website, *Cybersecurity Best Practices*, https://www.cisa.gov/topics/cybersecurity-best-practices, (accessed 4/4/24).
[11] Federal Bureau of Investigation website, *How We Can Help You*, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware, (accessed 4/4/24).
[12] J.P.Morgan website, *4 ways the public sector can prevent cyberattacks,* November 14, 2022, https://www.jpmorgan.com/insights/cybersecurity/business-email-compromise/threat-public-sector, (accessed 4/4/24).

DISCUSSION

The following discussion will examine the key elements of cybersecurity and cyber preparedness in Marin.

The Marin Department of Information Services and Technology (IST)

IST is responsible for providing, maintaining, and securing the County's business applications and data on the appropriate hardware and software platforms. IST "deploys information services and telecommunications technologies throughout the County government and maintains the County's technology infrastructure."[13]

The key responsibilities of IST are to:

- Support digital services that help our residents perform tasks online, like paying property taxes and getting building permits
- Support secure law enforcement and criminal justice systems
- Manage the County's geographic information and mapping systems
- Provide digital accessibility training and support to County employees
- Coordinate the cross-sector Digital Marin program
- Provide secure network and internet connectivity for County employees
- Manage and deliver technical projects that support Board and County priorities
- Support internal administrative systems for finance and human resources[14]

The IST web pages include one which details its Top 10 Cybersecurity Tips for Organizations. This webpage was last updated in November, 2023.[15] In addition, IST, in cooperation with the MSPC, sends out a monthly security awareness newsletter to Marin agencies and MSPC members, as well as alert notifications regarding active cyber threats. Through the Grand Jury's interviews with Marin's municipalities and agencies, it found that many were unaware of the security newsletter and the Top 10 Cybersecurity Tips available to them.

IST has also published objectives for Security Awareness[16] and Information Security.[17]

Within IST, the Information Security and Compliance (ISC) division is responsible for cybersecurity and is managed by the Chief Information Security Officer. Through interviews with IST staff, the Grand Jury has come to learn that IST has recently filled job positions in the cybersecurity area that had been open for a considerable time. This has been a difficult process

[13] County of Marin website, *Information Services and Technology*, https://data.marincounty.org/stories/s/s5cn-d5dy, (accessed 4/24/24).
[14] County of Marin website, *About the Information Services and Technology department*, https://www.marincounty.gov/departments/it/about-information-services-and-technology-department, (accessed 4/30/24).
[15] County of Marin website, *Top 10 Cybersecurity tips for organizations*, https://www.marincounty.gov/departments/it/cybersecurity/top-10-cybersecurity-tips-organizations, (accessed 4/24/24).
[16] County of Marin website, *Security Awareness*, https://data.marincounty.org/stories/s/Security-Awareness/9x7e-6eiy, (accessed 4/4/24).
[17] County of Marin website, *Information Security*, https://data.marincounty.org/stories/s/Information-Security/4mex-b65u, (accessed 4/4/24).

due to the following: high demand in the private sector for this skill, substantially lower salary levels in the county compared to the private sector, the high cost of living in Marin, and oftentimes considerable commute time. These problems affect all Marin agencies.

IST also sends out a monthly security awareness newsletter to member agencies of the MSPC for distribution to their employees. Employees receive alert notifications about active cyber threats requiring their attention, gain access to a document library with cybersecurity and digital privacy resources and templates, and have access to a peer network to ask questions and share ideas related to cybersecurity issues.[18] Unfortunately, in the Grand Jury's interviews with the heads of municipalities and special districts, there seemed to be an overall lack of awareness of the existence of the MSPC, as well as the Cybersecurity Tips. This may be due, in part, to the fact that the overall responsibilities of the ISC staff do not currently allow them sufficient time to reach out or collaborate through means other than email in order to better communicate with Marin Security & Privacy Council members.

Cybersecurity Best Practices

Municipalities

Through interviews and follow-up communications, the 2023-2024 Grand Jury studied each of Marin's municipalities to determine the status of implementation of the four primary, and additional four Cybersecurity Best Practices recommended in the 2019-2020 Grand Jury's report:

- Management of mobile devices
- Automated malware detection and removal
- Monitoring systems
- Use of expert resources
- Firewalls
- Hardware and patching
- Documentation
- Vulnerability assessments

The current Grand Jury found that 93 percent of the first four (the primary) recommendations had been implemented across all eleven municipalities. The remaining seven percent are in the process of being implemented. For the additional four recommendations, 90 percent have been implemented, while most of these four recommendations are in process.

The implementation of the eight best practices seems to have paid off. Since the 2019-2020 Grand Jury Report, none of the municipalities reported any material cyberattacks that would have been at the level of severity requiring public disclosure. Through interviews with members

[18] County of Marin News Release, C*yber Safety Group Opens to Marin Businesses*, May 19, 2022, https://www.marincounty.org/main/county-press-releases/press-releases/2022/ist-mscplaunch-051922, (accessed 4/4/24).

of the IST staff, the Grand Jury discovered that there were two cyberattacks reported by two other public agencies, but neither resulted in any material loss of data or money.

In interviews with each of the eleven municipalities, the most significant perceived cybersecurity risk is phishing. However, due to the implementation of regular cybersecurity training at their agencies, successful phishing attacks have been greatly reduced.

IST does not, nor is it required to, provide any additional cybersecurity assistance to Marin's municipalities (or special districts) other than the aforementioned newsletter and cyber alerts. In the Grand Jury's interviews the smaller municipalities in particular were receptive to additional collaboration and assistance from the County, due to staffing and budget constraints.

.GOV Domains

In November of 2023, Governor Newson signed into law AB 1637, requiring local agencies to migrate public websites and email addresses to a .gov or .ca.gov domain by January 1, 2029.[19] The law does not apply to special districts.

The .gov domain offers a secure way for internet users to identify and use legitimate government websites including multi-factor authentication. Also, browsers are required to use a secure internet connection to increase users' privacy on a .gov website. These safeguards help eliminate the clickjacking and spoofing of users visiting a .gov website. The Cybersecurity and Infrastructure Security Agency (CISA) manages the issuance of these domains. There is no cost to the public agency for registering a .gov domain.[20]

Of the 18 agencies investigated by the current Grand Jury, only one municipality, Sausalito, has fully transitioned to a .gov website. Sausalito took the initiative and completed their .gov website migration in 2017. The County and Marin's larger municipalities have begun rolling out .gov websites and have begun using .gov email addresses. However, the majority of the smaller municipalities interviewed or polled have no plans to either acquire a .gov domain name or to begin the process of moving to a new website platform using this domain. The relatively distant state-mandated time frame may explain why there has been a lack of movement here.

Other existing County .org domain names will be redirected to MarinCounty.gov as the websites are rebuilt. Educational institutions such as Marin schools are not eligible for .gov domains. They will be directed to use .edu domain names instead of their existing .org names.

The requirement of municipalities implementing a .gov domain is something to be kept in mind for all municipalities considering modifications of their current websites.

[19] California Legislative Information, California Law, California Government Code, Title 5, § 50034, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=50034.&article=, (accessed 4/24/24).
[20] Cybersecurity and Infrastructure Security Agency website, https://get.gov, (accessed 4/4/24).

Third-Party Providers of IT, IS and Cybersecurity Services

The Grand Jury discovered that many, if not all of the municipalities and special districts in Marin County, contract out their IT, IS and cybersecurity services to third parties due to a lack of either in-house expertise or budget. This is especially true for cybersecurity where few entities have the resources to design and implement their own solid cybersecurity defense.

Scope of Services

Third parties provide a broad set of cybersecurity-related services to the agencies the Grand Jury interviewed. These include cloud back-up, on-site support, remote monitoring, and end-point security, security awareness training, multi-factor authentication, mobile device management, and antivirus and anti-malware management. While this report does not question the quality of services provided by these third parties, there may be additional ways to provide cybersecurity services to the varied governmental agencies located in Marin County. See the discussion below on Joint Powers Authorities.

Monitoring Systems

Monitoring systems, often referred to as Security Information and Event Management (SIEM) systems, are cybersecurity solutions that help detect, analyze, and respond to security threats before they harm business operations. They are generally fully automated and operate 24 hours a day, seven days a week, 365 days a year. These systems however do not always remove or quarantine the cyber threat. Rather, notification of the cyber threat is sent to staff responsible for removing or quarantining the threat.

Through interviews with Marin agencies, the Grand Jury learned that staff response to agencies by the third-party providers on detected problems in the monitoring system is limited to typical office hours. Also, the contracts may only require *notice* to be delivered within 24 hours. Responding to cyberattacks needs to be handled immediately. Thus, agencies should work with their third-party providers to greatly reduce the amount of time between a detected cyberattack and the ability to isolate or eliminate the threat. Further, having multiple third-party entities servicing individual agencies does not offer the same benefit that a centralized system would provide by allowing experience gained addressing a particular threat to be applied across multiple potential targets.

Business Continuity Plans

A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. Such plans attempt to ensure that personnel and assets are protected and are able to function quickly in the event of a disaster, including cyberattacks. Most agencies that the Grand Jury investigated had their own BCP, or disaster recovery plan and procedures. The creation of a BCP is often at the recommendation of their third-party cybersecurity provider, or of the provider of their cyber insurance. However, in reviewing the contracts between the third parties and Marin agencies, the Grand Jury found no language in the contracts related to business continuity requirements *for any of the third-party providers*.

Requiring the third-party provider to have their own BCP is important as cyberattacks originating at trusted third parties are becoming more prevalent. Providing proof of liability insurance in the agreement is not enough. A recent report in *Security Scorecard*, stated that nearly thirty percent of cyber breaches come from third parties.[21] Threat actors are attracted to compromising third-party providers because of the high return on investment for these attacks - targeting one entity which provides access to multiple downstream clients.

Cybersecurity Plans

A cybersecurity plan is a comprehensive strategy that outlines measures to protect sensitive data, prevent cyber threats, and ensure the continuity of operations within an organization. Cybersecurity plans specifically help in preventing financial and personal data losses, ensuring data privacy, and protecting intellectual property. For smaller businesses and local government agencies, the Federal Emergency Management Agency offers a guide for organizations to plan, implement, and maintain a cybersecurity plan.[22]

From its interviews with Marin municipalities and special districts, the Grand Jury found that cybersecurity plans across these agencies varied widely in terms of completion and implementation. Several agencies have completed plans which are reviewed and updated regularly. Others are working on developing their plans either through their third-party IT and IS provider, or through their insurance risk pool.

Insurance Risk Pools, Cybersecurity Audits and Cyber Insurance

Grand Jury interviews with municipalities and special districts show that they receive their cyber insurance through insurance risk pools or risk management authorities. Many of Marin's agencies are members of the Bay Cities Joint Powers Insurance Agency (BCJPIA). This is one of several risk pools available in the Bay Area. It is used by most of the County's municipalities.

BCJPIA was created in 1986 to develop effective risk management programs to reduce the amount and frequency of losses; to share the risk of self-insured losses; and to jointly purchase and provide administrative and other services including, but not limited to, claims adjusting, data processing, risk management, loss prevention, accounting services, actuarial services, and legal services in connection with the program.

One of the services provided by the BCJPIA is a cybersecurity audit. The audit indicates areas requiring attention to maintain a functioning cybersecurity defense. These audits require individual members to respond to a series of questions concerning their IT systems and services. Items considered in the audit include the following:

[21] SecurityScorecard website, *Secure your supply chain*, p. 5, https://securityscorecard.com/wp-content/uploads/2024/02/Global-Third-Party-Cybersecurity-Breaches-Final-1.pdf, (accessed 4/4/24).
[22] FEMA website, *Planning Considerations for Cyber Incidents: Guidance for Emergency Managers,* November 2023, pp. 29-37, https://www.fema.gov/sites/default/files/documents/fema_planning-considerations-cyber-incidents_2023.pdf, (accessed 4/24/24).

- Upgrade legacy software and hardware
- Develop, implement, and improve a new password policy or current password policy
- Develop and implement a disaster recovery plan, business continuity plan, and incident response plan
- Include tabletop exercise(s) in the existing incident response plan
- Implement tools to help prevent email spoofing
- Provide security awareness training to all employees
- Initiate a network vulnerability scan
- Implement a security information and event monitoring (SIEM) tool

From its review of members audits by the BCJPIA and other insurance risk pool organizations, the Grand Jury found that the members had one or more deficiencies that required corrective action.

Joint Powers Authorities

The California State Legislature defines a Joint Powers Authority (JPA) as a stand-alone organization formed by governmental entities for a specific purpose or project. Two or more governmental entities can join together to form a JPA to solve mutual problems, to fund a project, or to act as a single representative entity for specific activities. A California agency can even share joint powers with an agency in another state.[23]

The primary purpose of forming a JPA is to enable public entities to pool resources. This could include the County agencies, municipalities, special districts, and other public agencies inside Marin. Pooling resources, coordinating efforts, and eliminating redundant actions or overlapping services can save taxpayer money. JPAs can also obtain more favorable rates or bids from outside services to achieve economies of scale.

Governmental entities can form a JPA to fulfill common objectives without voter approval or voter initiatives. However, these governmental entities must post notices, hold public meetings, and solicit comments from citizens or other stakeholders before executing any such agreements. Some of the more notable JPAs in the County include the Southern Marin Emergency Medical-Paramedic System (1980),[24] MARINet Libraries of Marin (1991),[25] Marin County Hazardous and Solid Waste - Zero Waste Marin (1996),[26] the Central Marin Police Authority (2013),[27] and the Marin Wildfire Prevention Authority (2020).[28]

To form a JPA, governmental entities must enter into a formal agreement. The agreement must identify a governing body, such as a Board of Directors and, in most circumstances, identify a

[23] California State Senate, Senate Governance and Finance Committee, *Governments Working Together: A Citizen's Guide to Joint Powers Agreements*, August 2007, p. 5, https://sgf.senate.ca.gov/sites/sgf.senate.ca.gov/files/GWTFinalversion2.pdf, (accessed 4/24/24).
[24] Southern Marin Emergency Medical Paramedic System, https://www.smemps.org, (accessed 4/4/24).
[25] MARINet Libraries website, https://marinet.lib.ca.us, (accessed 4/4/24).
[26] Zero Waste Marin website, https://zerowastemarin.org, (accessed 4/4/24).
[27] Central Marin Police Authority website, https://www.centralmarinpolice.org/, (accessed 4/4/24).
[28] Marin Wildfire Prevention Authority website, https://www.marinwildfire.org/collaborations/fire-adapted-marin, (accessed 4/4/24).

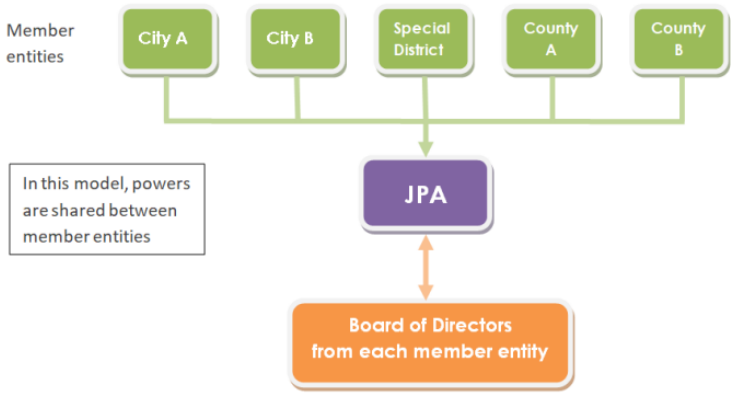
treasurer and an auditor. The agreement must be filed within 30 days of the effective date with the Secretary of State and the State Controller. There is no fixed timeframe to a JPA. Member agencies can choose to dissolve the JPA when it no longer serves their interests, or a predetermined termination date may be a part of the joint powers agreement.[29]

One form of a JPA is designed for insurance pooling and purchasing discounts. These JPAs usually involve governmental entities such as school districts or municipalities that need to buy insurance, supplies, or equipment. This type of JPA can also join with other insurance/purchasing JPAs to create a super JPA. These super JPAs can negotiate for lower rates and volume discounts for supplies, insurance, and equipment.

Most municipalities in Marin belong to an insurance pooling JPA as a way of reducing that municipality's overall insurance premiums, including cybersecurity insurance. These JPAs often offer their members annual audits of IT and IS security.

The structure of this type of JPA is usually a horizontal-model JPA. Horizontal-model JPAs consist of members that share a common opportunity, goal, or problem to solve. In general, they transfer their authority (with member entity representation) to a JPA to provide a service or fund a project. If the JPA is not performing well, not producing the desired results, or not delivering improvements, a member may withdraw.

Horizontal Model JPA Example



Source: Reprinted from *Joint Powers Authorities: What You Need To Know*
2020/2021 Nevada County Grand Jury Report Date: May 19, 2021

The Grand Jury observes that this type of Horizontal JPA would be the best choice for the formation of a cybersecurity JPA. The formation of such a JPA is consistent with the 2019-2020 Grand Jury's recommendation that "municipalities should pursue shared cybersecurity services, where feasible, to lower costs and raise their level of security."

[29] California State Legislature Senate Local Government Committee, *Governments Working Together, A citizen's Guide to Joint Powers Agreements*, August 2007, p. 26, https://sgf.senate.ca.gov/sites/sgf.senate.ca.gov/files/GWTFinalversion2.pdf, (accessed 4/29/24).

MIDAS

MIDAS is a consortium of government and nonprofit agencies within Marin. Its participants share this reliable and secure network infrastructure.[30] The members include numerous, but not all, municipalities located within the County, along with other public agencies. The MIDAS infrastructure includes internet connections at public buildings, access to law enforcement, emergency response and justice systems, and the ability to share data between agencies.[31] MIDAS serves government agencies and nonprofits. MIDAS provides access to reliable, secure, shared network services and manages the billing, support, and maintenance of the network infrastructure so that member agencies can focus their in-house resources on technology strategy and line-of-business applications.

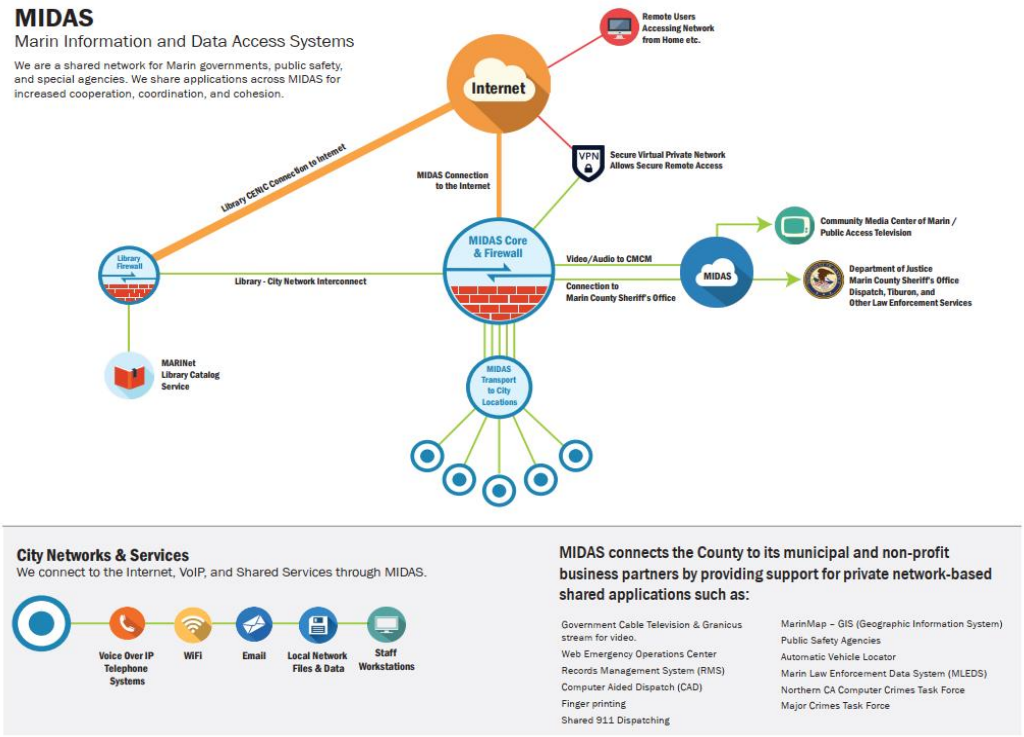
The County manages the funding and operation of MIDAS through the County's Information Services and Technology department. The County relies on charges to members to cover the cost of operations of the MIDAS network. There are two types of charges made to MIDAS members:

- MIDAS Service - for each MIDAS connection point
- Network Access - variable bandwidth charges for those MIDAS connections being used to access the internet

The MIDAS network infrastructure is maintained, through a professional services contract, by Marin IT, a private, third-party supplier of network services, founded in May of 2006. Its services range from as-needed to daily, full service support including project management, IT management, network management/administration, network monitoring, and help desk support. Through its contract, Marin IT provides managed network services up to the MIDAS router at each member remote location.

[30] Digital Marin website, Marin Information and Data Access Systems, https://godigitalmarin.org/marin-information-and-data-access-systems, (accessed 4/24/24).
[31] Digital Marin website, Marin Information and Data Access Systems, (accessed 5/9/24).

Configuration of the MIDAS Network



Source: County of Marin Department of Information Services and Technology

MIDAS originally included 21 members, spread amongst municipalities, nonprofits and special districts. As of the conclusion of the Grand Jury's investigation, MIDAS had 18 members, which are Marin County public agencies, as well as the Sonoma Marin Area Rail Transit (SMART). The set cost structure of MIDAS is shared on an equal basis by the members, while bandwidth charges are allocated on a "per-location" basis depending on the specific speed of each connection at the individual site. Over the years, some members who were using MIDAS other than for access to law enforcement, emergency response and justice systems, have chosen to leave MIDAS, because they were able to contract for equivalent bandwidth at less expensive rates than what is offered through their MIDAS membership. In addition, some municipalities who continue to use MIDAS for access to law enforcement, have either reduced or eliminated their non-law enforcement MIDAS connections. These changes have resulted in increases to the monthly charges to the remaining members of MIDAS due to the static fixed charge for the system being allocated among fewer constituents.

A review of the 2021-2022 County of Marin Annual Comprehensive Financial Report (ACFR), shows that MIDAS (referred to as 'Marin.org' in the report) was slightly profitable.[32] However, a copy of the draft 2022-2023 County Marin ACFR obtained by the Grand Jury, details that Marin.org's expenses were greater than its revenues. Finally, a review of IST's fourth quarter 2023 invoicing of MIDAS members for services, suggests that this cost differential may now be

[32] County of Marin website, *Annual Comprehensive Financial Report for the Fiscal Year Ended June 30, 2022*, p. 30, https://www.marincounty.org/-/media/files/departments/df/acfr/2022-county-of-marin-acfr_adagio_ada.pdf?la=en, (accessed 4/4/24).

even greater. Estimated revenues for calendar year 2023 appear to be less than $900,000, while expenses now appear to be significantly more than $1,000,000.[33]

One of the recommendations made in the 2019-2020 Grand Jury's report on cyberattacks was that The Marin County Information Services and Technology Department should complete a plan for enhancing MIDAS to improve cybersecurity for its users. As of the writing of this report, that plan has yet to be completed.

Collective Bargaining Agreements (CBA), Managed Service Agreements

In 1968, with the passage of the Meyers-Milias-Brown Act (MMBA), employees of cities, counties and special districts in California gained the right to form unions and collectively bargain contracts over changes in wages, hours, benefits, rights, and other terms of employment.[34] Two unions represent the County's IST's employees, the Marin Association of Public Employees (MAPE)[35] and the Marin County Management Employees Association (MCMEA).[36]

MAPE represents the vast majority of rank and file employees, while MCMEA represents about 350 mid-managers and supervisors across different County departments.

The current CBA with MAPE expires on June 30, 2026, while the MCMEA CBA expires on June 30, 2025. The agreements do not include language which would allow the IST or other County departments, the employees of which the two unions represent, to *unilaterally* negotiate managed service agreements (outsourcing work to third parties).

The CBA with MCMEA states that "Any work within the class specification for any classification currently represented by MCMEA shall not be contracted out during the lifetime of the contract without completion of the parties' meet and confer obligations or until negotiations for a successor agreement have concluded."[37] This language then allows for outsourcing; however, only through negotiation with either of the unions.

[33] Grand Jury work paper, *MIDAS Q4'24 Invoicing Reconciliation*, https://rebrand.ly/MarinCountyMIDASReconciliation, (accessed 4/4/24);
IST Flier describing some of the structure and responsibilities of MIDAS, as well as 2024 projected revenues and expenses, https://rebrand.ly/MarinCountyISTDeptMidasFlyer, (accessed 4/4/24).
[34] California Public Employment Relations Board website, *Laws*, https://perb.ca.gov/laws-and-regulations, (accessed 4/4/24).
[35] Marin Association of Public Employees website, https://www.newmape.org, (accessed 4/4/24).
[36] Marin County Management Employee's Association website, https://newmcmea.org, (accessed 4/4/24).
[37] Collective Bargaining Agreement Marin County Management Employees' Association County of Marin, July 1, 2022-June 30, 2025, p. 59, https://www.hr.marincounty.org/-/media/files/departments/hr/labor-relations/labor_agreements/mou--mcmea-20222025-for-web.pdf?la=en, (accessed 4/29/24).

The CBA with MAPE does not contain any language specific to contracting out work. However, the language in the MMBA, which governs such CBAs, does cover this (other than for custodial services).[38]

There is no prohibition of outsourcing for the purpose of changing the way services (that are currently being done by represented employees) can be done by a public entity, regardless of whether or not there is any flexibility or language in an CBA. However, the entity has to make sure the effects of the decision are properly negotiated with the union(s) if such outsourcing were to be done. If not, an unfair labor practice charge could be filed.

When the CBAs are renegotiated, it is vital that the County negotiate for expanded rights with respect to entering into managed-service agreements. Expanded rights for these types of agreements would allow IST to more easily contract for expanded cybersecurity services such as SIEM systems, Managed Detection and Response (MDR) or Endpoint Detection and Response (EDR). Additionally, the outsourcing of lower priority tasks such as desktop equipment deployment and support, would allow shifting and retraining of existing staff to higher priority, more strategic work. This retraining has the added benefit of allowing these employees to learn valuable new skills and be in a better position for career advancement in the cyber security area.

The Grand Jury has found that the level of cybersecurity preparedness has generally improved since the 2019-2020 Grand Jury report on cyber-attacks. However, due to the dynamic nature of the subject, this will require constant vigilance and investment in technologies.

[38] Collective Bargaining Agreement Marin Association of Public Employees General Bargaining Unit and the County of Marin, September 19, 2021-June 30, 2026, https://www.hr.marincounty.org/-/media/files/departments/hr/labor-relations/labor_agreements/mou--mape-gu-20212026--final-for-web.pdf?la=en, (accessed 4/30/24).

FINDINGS

F1. Contracts for Information Technology, Information Systems, and Cybersecurity services between third-party providers and Marin County governmental agencies should contain a Business Continuity clause, or other language, protecting that agency from a sudden cessation of services provided by the third-party provider.

F2. Marin County municipalities should have current, written contracts with third-party providers of Information Technology, Information Systems, and Cybersecurity services, and should not continue to use those providers' services without a current contract.

F3. Membership in insurance risk pools provides the benefits of cybersecurity assessments and audits, which highlight cybersecurity deficiencies and make suggestions for improvement.

F4. Having a completed, adopted and regularly updated cybersecurity plan helps ensure that all staff within a government agency are working together to optimize that organization's cyber preparedness and security.

F5. Joint Powers Authorities in Marin County exist to provide more efficient and cost-effective services to the people of Marin.

F6. The current County Collective Bargaining Agreements prevent the Marin County Department of Information Systems & Technology from unilaterally negotiating managed service agreements (outsourcing work to third parties).

RECOMMENDATIONS

The Grand Jury recommends that by December 31, 2024:

R1. Marin agencies should require a current (executed within the last five years), competitively-bid, written contract which includes business continuity language for any third-party Information Technology services they use.

R2. The Board of Supervisors should authorize the creation of a new position within the Department of Information Services and Technology for the 2025-2026 fiscal year, with specific responsibilities to assist other County agencies in cybersecurity awareness, training, implementation, and monitoring of cybersecurity systems.

R3. The Board of Supervisors should require that the Marin Department of Information Services and Technology evaluate the formation of a Cybersecurity Joint Powers Authority to raise overall cyber preparedness amongst its members, and for the purpose of acquiring and maintaining perimeter defense protection systems for preventing and eliminating ransomware and other more sophisticated cyberattacks.

R4. The Board of Supervisors should create two new system-engineering positions to be filled by cybersecurity experts who would be responsible for conducting security risk assessments, providing recommendations and implementing cybersecurity solutions for public agencies in Marin, among their other tasks.

R5. If and when a Joint Powers Authority is created, one of these positions would serve as a County member of the new organization and a liaison with the Chief Information Security Officer.

R6. All Marin municipalities should:

a) take all steps necessary to acquire an appropriate .gov or .ca.gov domain;
b) formulate and adopt a plan for rolling out a .gov or .ca.gov website and emails by the start of the 2025-2026 Fiscal Year.

R7. The Board of Supervisors should require that the Marin Department of Information Services and Technology:

a) develop a plan to redefine a secure network infrastructure of the MIDAS system which solely focuses on providing access to law enforcement, emergency response and justice systems, or other online County services, and exclude Internet Service Provider services;
b) take all steps necessary to transition administration of MIDAS from Marin IT to The County of Marin Department of Information Services and Technology.

R8. The Board of Supervisors require that the Marin Department of Information Services and Technology and the Department of Human Resources develop a plan for negotiating the inclusion of language that allows for managed service agreements in new Collective Bargaining Agreements with MAPE and MCMEA that will start in July of 2025.

R9. The Board of Supervisors requires that the Marin Department of Information Services and Technology update its Top 10 Cybersecurity Tips for Organizations at least once a year.

R10. The Board of Supervisors requires that the Marin Department of Information Services and Technology more directly promote, through the Marin Security and Privacy Council, its Top 10 Cybersecurity Tips for Organizations to all of Marin's public agencies.

REQUIRED RESPONSES

Pursuant to Penal Code section 933.05, the Grand Jury requires responses from the following governing bodies within 90 days:

- Marin County Board of Supervisors (F1-F6, R1-R6 (a) and (b), R7 (a) and (b), R8-R10)
- City of San Rafael (F1-F6, R1, R6 (a) and (b))
- City of Belvedere (F1-F6, R1, R6 (a) and (b))
- City of Larkspur (F1-F6, R1, R6 (a) and (b))
- City of Mill Valley (F1-F6, R1, R6 (a) and (b))
- City of Novato (F1-F6, R1, R6 (a) and (b))
- City of Sausalito (F1-F6, R1, R6 (a) and (b))
- Town of Corte Madera (F1-F6, R1, R6 (a) and (b))
- Town of Fairfax (F1-F6, R1, R6 (a) and (b))
- Town of Ross (F1-F6, R1, R6 (a) and (b))
- Town of San Anselmo (F1-F6, R1, R6 (a) and (b))
- Town of Tiburon (F1-F6, R1, R6 (a) and (b))

The governing bodies indicated above should be aware that the comment or response of the governing body must be conducted in accordance with Penal Code section 933 (c) and subject to the notice, agenda and open meeting requirements of the Brown Act.

INVITED RESPONSES

- Marin County of Marin Department of Information Services and Technology (F1-F6, R2-R4, R6 (a) and (b), R9)
- Marin County Department of Human Resources (F6, R8)

Note: At the time this report was prepared information was available at the websites listed.

Reports issued by the Civil 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 Civil Grand Jury. The California State Legislature has stated that it intends the provisions of Penal Code Section 929 prohibiting disclosure of witness identities to encourage full candor in testimony in Grand Jury investigations by protecting the privacy and confidentiality of those who participate in any Civil Grand Jury investigation.

APPENDIX A

Cybersecurity Terms and Definitions

Adversary/Threat Actor: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Antivirus software (AVS): A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents and sometimes by removing or neutralizing the malicious code.

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Cybersecurity and Infrastructure Security Agency (CISA): Is responsible for developing a range of cyber and infrastructure security services, publications, and programs for the federal government, state, local, tribal, and territorial (SLTT) governments, industry, small and medium-sized businesses, and the general public. CISA defends critical infrastructure against threats and assists both other government agencies and private sector organizations in addressing cybersecurity issues.

Clickjacking: Involves tricking someone into clicking on one object on a web page while they think they are clicking on another. The attacker loads a transparent page over the legitimate content on the web page so that the victim thinks they are clicking on a legitimate item when they are really clicking on something on the attacker's invisible page. This way, the attacker can hijack the victim's click for their own purposes. Clickjacking could be used to install malware, gain access to one of the victim's online accounts, or enable the victim's webcam.

Cybersecurity: Relates to the processes, computer hardware and software employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. Cybersecurity requires extensive knowledge of possible threats such as viruses or other malicious objects. Identity management, risk management, and incident management form the crux of the cybersecurity strategies of an organization.

Dark Web: The Dark Web is encrypted parts of the internet that are not indexed by search engines, most notoriously used by all types of criminals including; pedophiles, illicit human and contraband traffickers, and cyber criminals, to communicate and share information without being detected or identified by law enforcement. Malware of all types can be purchased on the dark web. Dark Web pages need special software with the correct decryption key and access rights and knowledge to find content. Users of the Dark Web remain almost completely anonymous due to its P2P network connections which makes network activity very difficult to trace.

Data breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Denial of Service: An attack that prevents or impairs the authorized use of information system resources or services.

Distributed Denial of Service (DDOS): A denial of service technique that uses numerous systems to perform the attack simultaneously.

Endpoint Detection and Response (EDR): Also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

Firewall: A Firewall is a security system that forms a virtual perimeter around a network of workstations preventing viruses, worms, and hackers from penetrating.

Information Systems (IS) is a term for how data is collected and used in an organization including the hardware, software and network communications.

Information Technology (IT) is a common term typically for aspects related to business enterprise computing including hardware, software and infrastructure.

Interactive Intrusion Techniques: Malicious activities where an Adversary actively interacts with and executes actions on a host to achieve their goals. Unlike automated Malware attacks that rely on the mass deployment of scripts and tools, interactive intrusions leverage the ingenuity and problem solving skills of human adversaries. These individuals can mimic expected user and administrator behavior, making it difficult for defenders to differentiate between legitimate user activity and a cyberattack.

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

Managed Detection and Response (MDR): A (third-party) cybersecurity service that provides organizations with a team of experts who monitor your endpoints, networks and cloud environments and respond to cyber threats 24/7.

MIDAS is a consortium of government and nonprofit agencies within Marin County. It provides a reliable and secure network infrastructure.

Multi Factor Authentication (MFA): A form of authentication that requires a user to provide two or more verification factors to access a resource such as an online account.

Phishing: Phishing is a type of internet fraud that seeks to acquire a user's credentials by deception. It includes the theft of passwords, credit card numbers, bank account details, and other confidential information. Phishing messages usually take the form of fake notifications from banks, providers, online payment systems, and other, legitimate-looking organizations. The phishing attempt will try to encourage a recipient, for one reason or another, to enter/update personal data. Common reasons given can include "suspicious login to the account," or "expiration of the password."

Ransomware: Is the name given to malicious programs designed to extort money from victims by blocking access to the computer or encrypting stored data. The malware displays a message offering to restore the system/data in return for payment.

Security Information and Event Management (SIEM): A cyber security solution that helps organizations detect, analyze, and respond to security threats before they harm business operations. SIEM combines both security information management (SIM) and security event management (SEM) into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.

Spoofing: A Spoof is an attack attempt by an unauthorized entity or attacker to gain illegitimate access to a system by posing as an authorized user. Spoofing includes any act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address.

Third-party relationship exploitation: This type of cyberattack takes advantage of vendor-client relationships to deploy malicious tooling via two key techniques: 1) compromising the software supply chain using trusted software to spread malicious tooling and 2) leveraging access to vendors supplying IT services.

Zero Trust Architecture: Zero Trust Architecture is a security concept centered around the idea that organizations should not automatically trust anything inside or outside of their perimeters and instead must verify anything and everything trying to connect to their systems before granting access. This approach is based on the principle of "never trust, always verify." Zero Trust Architecture operates on the assumption that threats exist both inside and outside the network, and it focuses on maintaining strict access controls and continuously verifying the trustworthiness of users and devices. This is done through various methods such as multi-factor authentication, micro-segmentation, least privilege access, and continuous monitoring of network traffic and user behavior.