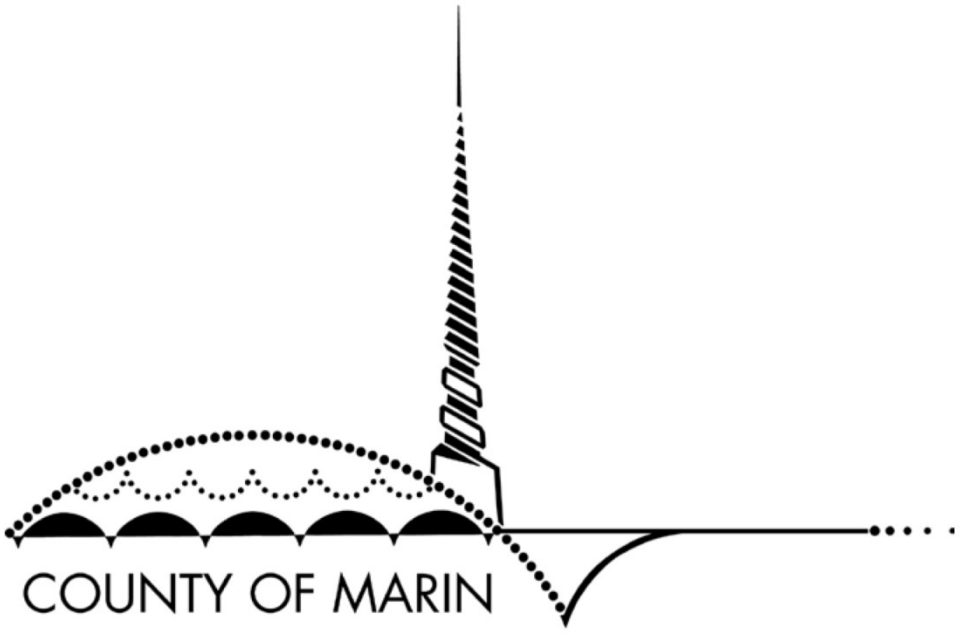
2019–2020 MARIN COUNTY CIVIL GRAND JURY

Cyberattacks: A Growing Threat to Marin Government

May 11, 2020



A Note about the Coronavirus Pandemic

The 2019–2020 Marin County Civil Grand Jury is issuing its reports during the unprecedented conditions of the COVID-19 pandemic. We are well aware that Marin County is in crisis and that critical public health concerns, operational difficulties, and financial challenges throughout the county have a greater claim to government attention right now than the important issues raised by this Grand Jury.

We are confident that, in due course, Marin will come through this crisis as strong as ever.

Cyberattacks: A Growing Threat to Marin Government

Summary

Local governments are targets of opportunity for cybercriminals. Hackers seek unauthorized access to computer networks so they can install ransomware, steal personal information, benefit from fraudulent payments, and disrupt government operations. As our government agencies become more reliant on online systems and remote work capabilities, cybersecurity awareness and best practices are increasingly critical.

Unbeknownst to the public, the Marin County government and most of Marin's municipalities have suffered financial frauds or debilitating network breaches in recent years. The county lost almost $250,000 in a wire fraud scheme in 2018. More than half of Marin's 11 cities and towns—Corte Madera, Fairfax, Larkspur, Novato, Sausalito, and Tiburon—have fallen victim to successful breaches, and these are just the ones disclosed to the Marin County Civil Grand Jury.

Our government leaders have not disclosed most of these incidents to other Marin agencies or the public, leaving us underinformed and underprepared.

The Grand Jury's recommendations include the following:

- 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.
- The county and each city and town council should hold public discussions, at least annually, on their cybersecurity measures, which would also raise awareness among residents and local organizations on ways to improve cybersecurity.
- If the county or a municipality experiences a breach, it should promptly notify federal law enforcement and disclose the breach publicly.
- Municipalities should pursue shared cybersecurity services, where feasible, to lower costs and raise their level of security.

The Grand Jury focused its investigation on the security of the computer systems used by Marin's county and municipal governments. This investigation did not attempt to assess the cybersecurity posture of other Marin agencies, but the Grand Jury recommends that all of them undertake a comprehensive review of their cybersecurity practices, if they have not done so already.

Background

In May 2019, hackers seized control of the City of Baltimore's computer networks and demanded an $80,000 ransom to restore staff access. The city refused to pay it, and operations were paralyzed for several weeks as technicians attempted to restore the network. Taking into

account lost revenue and the cost to rebuild the system, the attack cost Baltimore's taxpayers an estimated $18 million.[1]

The successful attack on Baltimore's computer system was just one of at least 70 ransomware attacks on U.S. state, county, and local governments during the first 8 months of 2019. Because of underreporting, the total number of such attacks may have been much higher. The size of the target does not matter—many of the ransomware attacks analyzed in 2019 took place in towns with fewer than 15,000 residents.[2] Hackers know that smaller municipalities can be easy targets because of inadequate network protections and spotty adherence to best cybersecurity practices, and these criminals are expected to increase their assaults on them.[3]

But government computer systems can be vulnerable to more than just ransomware attacks. As shown in the box below, cyberattacks can take many forms. The threats and tactics used by hackers evolve constantly. During 2019, the FBI received more than 460,000 complaints of internet crime from individuals and organizations throughout the United States, with reported losses totaling more than $3.5 billion. Nearly half of the losses resulted from hackers duping email recipients into clicking on or responding to fraudulent emails.[4] In the Bay Area, a computer virus infected Union City's systems for several days in September 2019, crippling the

Common Types of Cyberattacks

- **Direct attack**: A direct attack is where a hacker seeks to use a stolen password or exploit a weakness to gain direct access to a private network to steal data or crash the system.
- **Ransomware**: In a ransomware attack, a hacker installs software that encrypts the data or crashes the system, preventing the owner from accessing applications or data. The hacker demands a ransom in exchange for unlocking the system and restoring the data.
- **Phishing**: Phishing involves a hacker sending an email or text message designed to trick the recipient into divulging personal or sensitive information, such as a password or Social Security number. Research has shown that more than 90 percent of cyberattacks start with phishing emails. Some phishing emails use a forged sender's address (pretending, for example, to be from a senior leader in a government agency), requesting the user to click on a link that might install malicious code, to transfer money or make a payment to a fake third-party account controlled by the hacker, or to reveal sensitive information.

[1] Ian Duncan, "Baltimore Estimates Cost of Ransomware Attack at $18.2 million as Government Begins to Restore Email Accounts," *Baltimore Sun,* May 29, 2019, https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.
[2] Barracuda Blog, "Threat Spotlight: Government Ransomware Attacks," August 28, 2019, https://blog.barracuda.com/2019/08/28/threat-spotlight-government-ransomware-attacks/.
[3] Allan Liska, Recorded Future, *Early Findings: Review of State and Local Government Ransomware Attacks*, May 2019, https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf.
[4] Federal Bureau of Investigation, *2019 Internet Crime Report*, February 2020, pp. 5, 9, https://pdf.ic3.gov/2019_IC3Report.pdf.

city's email system, payment and financial systems, business licensing system, and planning and building permit and licensing systems.[5]

A 2016 survey of chief information officers of U.S. municipal and county governments by the International City/County Management Association showed the following:[6]

- 44 percent reported being subjected to an attack at least once a day, where an attack is "an attempt by any party to gain unauthorized access."
- 25 percent reported at least one incident monthly, which led to a compromise to the "confidentiality, integrity, or availability of an information asset."
- 24 percent reported at least one breach annually, which resulted in confirmed, unauthorized disclosure of information to a third party.

Staying secure requires vigilance and adaptability. Given the increasing threat of cybersecurity attacks, it is incumbent upon governmental organizations of all sizes to assess and, where needed, strengthen their networks against cyberattacks in order to protect the data of citizens and employees, to ensure the uninterrupted functioning of local governmental agencies, and to safeguard important infrastructure.

Approach

In its investigation of cybersecurity in Marin, the Grand Jury:

- Interviewed representatives from the county government, as well as representatives from each of Marin's 11 towns and cities
- Interviewed members of the Marin Managers Association
- Interviewed a member of the Marin County Council of Mayors & Councilmembers
- Reviewed articles, surveys, and research papers concerning information security practices and the use of shared services arrangements in local governmental agencies

The Grand Jury chose to focus on cybersecurity practices at the county and municipal level. This investigation did not attempt to assess the cybersecurity posture of the various school districts, law enforcement agencies, water agencies, sanitation districts, and other special districts.

The Grand Jury also investigated the county's election system. Election security in the county appears to be strong and well-organized. The county's Elections Department runs all federal, state, county, city, school, and district elections held in the county. Election procedures are mandated at the state and federal level. Marin's voter-management computer system is provided

[5] Union City, "Update: Computer Virus Continues to Impact Online Services," news release, September 23, 2019, https://www.unioncity.org/CivicAlerts.aspx?AID=69; Anna Bauman, "Computer Virus Wreaks Havoc on Union City's Municipal Servers," *San Francisco Chronicle*, September 23, 2019, https://www.sfchronicle.com/bayarea/article/Computer-virus-wreaks-havoc-on-Union-City-s-14461096.php.

[6] International City/County Management Association, *Cybersecurity 2016 Survey*, 2016, p. 6, https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf.

by a state-certified outside vendor. Paper ballots are used rather than voting machines, and the computers used for vote counting are never connected to the internet.

Discussion

Government in Marin County needs strong, effective cybersecurity measures to protect its information, operations, and assets.

Little-Known Breaches Have Harmed Marin's County and Municipal Governments

Imagine that Jamie, an employee in the finance department of a county government, receives four emails from Drew, a coworker in another department, requesting wire transfers into several bank accounts. Jamie does not notice that the emails are fake and transfers more than $300,000 as requested. Or imagine that Casey, an employee responsible for payroll in a city government, receives an email from the city manager requesting copies of the W-2 tax forms of all city employees and councilmembers. Casey also does not detect that the email is fake and unwittingly sends the tax forms to a hacker, who then files at least three fraudulent tax returns. Except for the names of the government employees, these disturbing scenarios actually occurred. They occurred in 2018. And they occurred in Marin.

In the course of this investigation, the Grand Jury learned that the Marin County government's computer network was breached at least five times in the past few years, and more than half of Marin's cities and towns also were successfully attacked.

A Wake-Up Call for the County

The county government's main computer network is managed by its Information Services and Technology Department (IST) and serves all county departments.

County officials reported to the Grand Jury that they have not experienced a successful, disabling ransomware attack during the last three years. However, from July 2017 through August 2018, the county suffered at least five cyberattacks that compromised system security. Mostly a result of phishing attacks, these breaches resulted in the successful theft of employees' login credentials, potentially enabling the perpetrator to log in to the county's network to steal data or install malware. In four of these breaches, according to information provided to the Grand Jury, there was no evidence of actual data theft.

But the fifth breach was different. After receiving a phishing email in April 2018, a county employee clicked on a link that allowed the hacker to access and control the employee's email account. The hacker was then able to review emails that detailed the procedures for requesting wire transfers of funds, change the email account settings so the employee would not detect what the hacker was doing, and send an email in the employee's name to the county's finance department requesting a $78,000 wire transfer. A finance employee processed the request and initiated the wire transfer.

Over a one-week period in late April, the hacker repeated the same fraudulent scheme three more times. In all, the finance department wired $309,000 to the hacker's bank accounts. After detecting the fraud, the county was able to recover approximately $63,000, leaving a total loss of $246,000. This breach and financial loss were reported to local law enforcement and the FBI, but not disclosed to the public.

In the wake of these incidents, the county government instituted numerous changes to reduce its vulnerability to attacks on its networks. Some of these were technical changes, such as making it impossible to automatically forward emails to outside the county's network, and blocking connections from outside the United States.

With the help of both external and internal auditors, the department of finance reexamined its internal controls, audited all wire transfers for the preceding 12 months, and identified and immediately implemented process improvements to mitigate the risk of fraud and misappropriation of assets. The department's management also counseled and issued formal warnings to the employees who were deceived by the fraudulent requests.

Other changes involved new personnel and programs in the Information Services and Technology Department. In May 2018, the county hired a new Chief Information Officer, who quickly expanded the size of the information security team and created the position of chief information security officer. Among other measures, that team developed a program, called People at the Heart of Information Security, to create a security-minded culture throughout county government. The program includes mandatory user training regarding cyberattacks, the addition of a "Phish Alert" button to allow employees to report suspicious emails, mock phishing exercises, brown-bag security awareness sessions, and other activities. In 2019, the California State Association of Counties awarded Marin County a Challenge Award for this effort.[7]

The Grand Jury concluded that the county now has a well-developed approach to cybersecurity in general and a robust architecture and strategy for avoiding hacks, including ransomware attacks. The county's data backup and hardware redundancy strategy appears strong, which should enable IST to recover quickly from a disabling attack should one occur. IST also takes advantage of outside resources, such as those provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC) within the Department of Homeland Security's Center for Internet Security. MS-ISAC specifically focuses on state and local governments, and it provides free services and tools to help them improve their cybersecurity.[8]

Still, there is more that the county government can do to ensure the security of its systems, and county officials informed the Grand Jury that efforts are ongoing to make the county's systems even more secure.

[7] California State Association of Counties, "2019 Challenge Awards Recipients," 2019, https://www.counties.org/post/2019-challenge-award-recipients.

[8] Center for Internet Security, MS_ISAC, accessed April 15, 2020, https://www.cisecurity.org/ms-isac/.

The Vulnerability of Marin's Cities and Towns

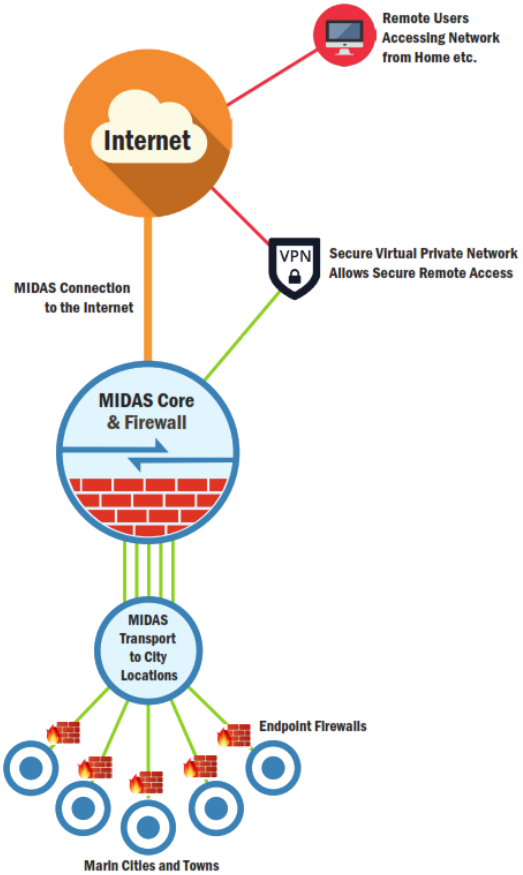
Each of Marin's 11 incorporated cities and towns has its own network, and most of these municipalities rely on contractors for information technology (IT) support. Although they have separate IT systems, the county government and all the municipalities, except Corte Madera, share a wide area network known as the Marin Information and Data Access System (MIDAS). This shared network, which is depicted in Figure 1, is managed by the county government together with an outside vendor. MIDAS provides its users with a secure connection to the internet and also enables them to share certain applications hosted at the county level. A firewall at each endpoint on this system minimizes the risk of a direct attack by an outsider, but MIDAS does not currently protect against all types of attacks. Attacks that use fake emails as their entry point are not stopped, nor does MIDAS currently provide malware filtering or antivirus protection.

The Grand Jury found that information security practices in Marin's cities and towns are deficient by several measures, especially if one measures security by the number of breaches that have occurred. Six cities and towns disclosed to the Grand Jury that they were successfully attacked over the last four years. Three of the breaches were ransomware attacks. The breaches disabled computers and network systems, resulted in financial fraud, and led to the theft of confidential information:

Town of Fairfax: In July 2016, Fairfax was victimized by a ransomware attack. An employee received an email with a malware program attached; and when the employee clicked on the attachment, the town's servers were infected and became unusable. No ransom was paid, but the town was forced to use a previous backup in order to rebuild its systems. The town lost data for the day of the attack, since it had not yet been backed up. Fairfax suffered a similar breach in October 2014.

City of Novato: In 2017, Novato fell victim to a phishing attack. A city employee received an email purporting to be from a senior city official, requesting a wire transfer of funds. The employee initiated the wire transfer to the account specified by the hacker. The Grand Jury received two conflicting reports regarding

Figure 1. MIDAS Shared Network



Note: This diagram has been simplified and does not show connections to the county library, sheriff's office, and other agency networks.
Source: Adopted with changes from Marin County Information Services and Technology Department, *What Is MIDAS?*, July 2018.

this breach. In one telling, the wire transfer was approximately $15,000 and much of the money was later recovered. In the second version, approximately $40,000 was wired and none of it was recovered by the city. The breach was reported to local law enforcement and the FBI. Due to extensive turnover among the Novato city staff, the Grand Jury was unable to determine the exact amount of the financial loss. After the attack, Novato strengthened its email security and implemented mandatory employee training to reduce its vulnerability to email-based attacks.

City of Sausalito: In January 2018, Sausalito was the victim of a phishing attack in which a fake email, purporting to be from the city manager, was sent to a city employee. This employee complied with the fake email's request for copies of the W-2 tax forms of all of the city's employees and councilmembers. As a result, all these individuals were exposed to the risk of identity theft. The Sausalito breach was reported to the FBI. For two years after the attack, the city provided free credit monitoring services to all employees, at a cost of approximately $27,000. Nevertheless, three employees had fraudulent state tax returns filed in their names, although the attempts were unsuccessful because taxing authorities had been alerted.

Town of Tiburon: In 2019, Tiburon suffered a ransomware attack, also initiated by a fake email attachment opened by an employee. No ransom was paid, but the town's systems were largely disabled for more than three days. Most of its data was recovered using a backup, but the town discovered that one of its applications was not being backed up properly, so the town needed to rebuild much of that data by hand from paper records.

Town of Corte Madera: In 2019, Corte Madera suffered a direct attack. During a brief moment when a vendor intentionally disabled the town's firewall for system updates, hackers were able to access its network and disable it using ransomware. No ransom was paid, but the system had to be restored from a backup.

City of Larkspur: In August 2019, Larkspur's network was compromised in a direct attack. Four of its computers were reportedly accessed from one of the public computers in the Larkspur library. It is unknown what data may have been accessed.

Observations

The Grand Jury was able to make several observations about these successful cyberattacks on Marin's county and municipal governments:

- Email-based attacks succeed due to poor user behavior and can be greatly reduced by training to instill good user behavior.
- The MIDAS platform does not prevent email-based breaches or filter for viruses.
- To the Grand Jury's knowledge, the county breaches and the $246,000 loss were never disclosed publicly, and the only municipal breach that became known to the general public was Sausalito's. By not being sufficiently informed about the cybersecurity risks that exist in our cities and towns, the public may have a false

sense of security regarding effective government operations. Public transparency is essential so that Marin residents are aware of cybersecurity risks.

- While the Sausalito and Novato breaches and one of the county breaches were reported to the FBI, the Grand Jury was unable to determine whether the other incidents were reported to federal law enforcement. The FBI recommends that government agency breaches be reported as a standard practice.[9] In addition, when unauthorized disclosure of personal information occurs, California law requires the agency to notify all affected individuals, as Sausalito did in this case.[10]
- Sausalito, according to interviews, responded appropriately to its breach. It not only notified the FBI, but provided identity theft protection resources to its employees, held a city council discussion on cybersecurity, and implemented a number of measures to strengthen its security, including mandatory employee training, technology for flagging external emails, and ongoing monitoring of its system by a cybersecurity consultant.
- Partly as a result of the breaches to its systems, the county has acquired expert knowledge about techniques and strategies to prevent breaches and is in a strong position to share that expertise with cities, towns, and other agencies in Marin that may lack access to such practical knowledge.

City and Town Officials Are Not Sufficiently Engaged in Combating Cyberattacks

In municipalities across the United States, cybersecurity awareness and support for a stronger approach from elected representatives and top officials appear to be lacking. In 2016, the International City/County Management Association surveyed the chief information officers (CIOs) of U.S. county and city governments regarding cybersecurity issues. The survey asked the CIOs about the engagement of their top appointed or elected officials in cybersecurity risks and found, among other things, the following:[11]

- Only 26 percent of the CIOs believed that elected council members were either moderately or exceptionally aware of cybersecurity issues.
- Only 30 percent of the CIOs reported that elected council members provided either strong or full support for cybersecurity.
- According to the CIOs, a very low percentage of elected and appointed officials felt they personally had a strong responsibility for cybersecurity.

The survey results indicate that, while there is some awareness about cybersecurity risks, there is a lack of engagement by local elected officials in ensuring strong security. Marin is no exception

[9] FBI, *Law Enforcement Cyber Incident Reporting*, accessed April 15, 2020, https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view.
[10] California Civil Code § 1798.29, accessed April 15, 2020, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29.
[11] International City/County Management Association, *Cybersecurity 2016 Survey*, pp. 3, 12.

to the survey findings. As the above discussion of past attacks in Marin noted, city and town councils have not taken up the cause to raise public awareness or to combat cyber risks. In most cases, information security is an operational issue delegated to the town or city manager. In those municipalities suffering a breach, the Grand Jury found only one instance—Sausalito—where a city council directed its manager post-breach to provide the council with an assessment of its cybersecurity practices or measures that could be taken to improve security.

While city and town managers in Marin are generally aware of the increasing number of cyberattacks, there appears to be a lack of action on the issue. In the course of its investigation, the Grand Jury heard repeated comments similar to the following:

- *Since we have a full backup, we are not too concerned about losing data* (this, despite the fact that restoration of an untested backup might fail and an attack could cause loss of the current day's data and an interruption in government operations lasting several days or more). There appears to be an overconfidence in the ability of a backup to enable a municipality to recover rapidly from an attack.
- *Our data is mostly a matter of public record anyway, so we are not too concerned about public disclosure* (in fact, much of their data is confidential, including human resources data and information about pending litigation, not to mention information about private citizens that could be used in identity theft). There appears to be insufficient concern about the government's need to protect important, confidential information.

The Public Is Underinformed about Cybersecurity Threats to Our Government

None of the breaches described above (other than the Sausalito attack) resulted in any public discussion by the governing boards of cyber threats or a demand from the board that the manager report to it regarding steps being taken to reduce those risks. The absence of a public discussion of these vulnerabilities is a missed opportunity to educate employees, residents, and local organizations about the cybersecurity risks faced by all.

The Grand Jury heard two separate views on the wisdom of discussing these matters publicly. The first is that public disclosure would alert potential hackers that a jurisdiction is vulnerable to an attack. The second view is that, by disclosing and openly discussing the problem, coupled with taking strong action to improve network security, the jurisdiction makes clear its commitment to a high level of vigilance and security and reduces its attractiveness to potential hackers.

While it would never be prudent to disclose in detail any technical vulnerabilities that led to a breach, the fact is that most attacks are launched when an employee clicks on a malicious email, and disclosing such an incident would not increase a municipality's vulnerability but could serve to educate employees and residents of the importance of good user behavior. Unless disclosure would clearly create new security risks, the Grand Jury strongly favors public disclosure of these incidents.

Our Cities and Towns Should Adopt Best Practices to Improve Security

A strategy followed by many smaller private and public organizations is to adopt "best practices" identified by IT professionals as a way of ensuring that they keep up with constantly changing risks.[12] The Grand Jury investigated industry-standard best practices, as well as practices implemented successfully by various Marin agencies, and this report recommends that a number of them be implemented by all cities and towns in Marin.

The National Institute of Standards and Technology has created its Cybersecurity Framework to assist governmental agencies and others with their security planning and practices. It identifies five key steps to planning and implementation: identify, protect, detect, respond, and recover.[13] All public officials and managers should become familiar with its guidance and principles.

Smaller cities and towns may believe that they cannot afford stronger security. However, the Grand Jury concluded that there are a number of inexpensive measures that every municipality should implement, if they have not done so already, that would materially strengthen their security.

Employee training

User behavior is at the center of cyber vulnerability and poses one of the greatest security challenges because it is difficult to change. Phishing attacks are initiated by email. They exploit employee behavior to gain network access. The more aware users are of hacking tactics, the better able they will be to avoid attacks—whether they are working in the office or at a remote location. The Grand Jury recommends regular, *mandatory* employee training to educate, motivate and, yes, scare, employees into following security practices. (One manager informed the jury that employees should feel "terrified" about what could happen in an attack.)

One technique is to send fake emails to employees on a random basis to identify which employees have poor security discipline so that those employees can receive more training and more controlled network access. The jury recommends a service like this for all municipalities.

Email Flagging and Filtering

Malicious emails are often disguised to appear as if they came from within the organization, tricking the user into believing the email is from a colleague. To help counter this deception, the email system should place a visible "flag" on any email sent by someone from outside the organization. The County of Marin and several Marin cities and towns have already implemented such a system, but not all. Those that have done so report that the flag system has greatly improved user behavior. For a higher level of protection, the organization could implement a

[12] Ekran System, "12 Best Cybersecurity Practices in 2020," https://www.ekransystem.com/en/blog/best-cyber-security-practices; MetroStar Systems, "13 Cybersecurity Best Practices You Should Apply in 2020," https://www.metrostarsystems.com/cyber-security/13-cybersecurity-best-practices-apply-2020/; ObserveIT, "10 Essential Cybersecurity Best Practices for 2019," https://www.observeit.com/blog/10-essential-cybersecurity-best-practices-for-2019/.

[13] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

system, as Sausalito has done, that will not deliver an email until the recipient verifies that the actual email address of the sender is the same as the purported address.

All email systems should also have filters, sometimes called spam filters, that identify suspicious emails. Rather than letting these emails be delivered, the system "quarantines" them (or it may delete some emails entirely, depending on the security settings). The intended recipient receives a daily email listing all the quarantined emails and can then opt to have the emails he or she deems safe to be delivered. The rest are deleted. The Grand Jury recommends that all Marin cities and towns not only have such filters on their email systems, but also use the highest security settings available, consistent with operational needs.

Password Management

Strong, enforced password policies are essential to network security. If users create easy-to-guess or weak passwords, hackers can easily gain access. Password policies should require users to use complex passwords (using uppercase and lowercase letters, numbers, and special characters), to avoid sharing passwords or using the same password on multiple systems, and to change passwords periodically, at least every six months. With most systems, these policies can be enforced automatically by the system.

User accounts also need to be managed tightly. When an employee leaves the organization, the account should be disabled immediately. In addition, many employees are given access to ancillary accounts, such as the municipality's website, its social media accounts, its wifi network, and other cloud-based systems. The organization should create documented security procedures to inventory all of these other user accounts and ensure conformity with password policies.

Organizations should be encouraged to use "password managers" where feasible. A password manager is a software program that performs like a vault to store all of your passwords and automatically log you in to a website where you have an account. By making password managers available to staff, the agency enables users to create very complex passwords that do not need to be memorized and to use different complex passwords on every system that they access.

System administrators should also consider deploying "two-factor authentication" in certain cases. In addition to requiring the user to enter a password, this security feature requires the user to provide a second security credential before getting access. Most people have experienced this when they receive a text message containing a special code that must be entered before they can log on to a website. Two-factor authentication certainly should be used to access laptops and other mobile devices. It should also be required when accessing the system from outside the network.

Data and System Backups

Backups make a copy of the data on a computer or server to an alternative location to enable recovery from a data loss or a system lockup. Data should be backed up at least daily, although some systems allow data to be backed up throughout the day, which is better. Server backups should be made regularly to enable servers to be restored entirely from scratch to recover from ransomware attacks and similar outages.

While it is easy to set up a system for regular backups, the system should be tested regularly to confirm that the data can actually be restored. Backups are notorious for failing. Backups should be monitored for failure, and testing should be done at least monthly. The Grand Jury's interviews revealed that city and town officials generally do not know whether their backup systems are ever tested.

Other Best Practices

There are a variety of other best practices that all cities and towns should evaluate for implementation, including these:

- **Management of mobile devices**. Phones, tablets, laptops, and other mobile devices pose special risks because they are more susceptible to being lost or stolen. An agency should either prohibit the use of mobile devices to access government data or ensure that it has a platform to manage mobile devices. This system should include (1) enabling password management controls, (2) requiring two-factor authentication, (3) requiring use of a virtual private network, (4) encrypting all information stored on the mobile device, and (5) enabling "remote wipe" so that when a device is lost, its data can be deleted remotely.
- **Automated malware detection and removal**. Antivirus software on the servers and personal computers can detect and remove malware before it does any damage.
- **Monitoring systems**. Despite best efforts, most systems will end up being penetrated. It is important to have a monitoring system enabling the manager to see what is happening on the system and be alerted immediately when hackers have gained access.
- **Use of expert resources**. Cyber threats are constantly evolving, and it is difficult for the average IT professional to stay current. It is critical to have access to an expert outside resource, especially when performing vulnerability assessments. Free resources such as the MS-ISAC alerts and newsletters can keep city and town managers (or their outside consultants) aware of new threats and risk-reduction techniques.
- **Firewalls.** A firewall is a hardware device or software element that can block and filter outside access to a network. Firewalls should be up to date and deployed with security settings that are as strong as feasible, blocking, for example, all access from outside the United States.
- **Hardware and patching**. Many attacks happen because older computer operating systems are no longer supported and cannot be patched with up-to-date software. It is common to replace computers every three to four years to minimize this problem. Grand Jury interviews revealed that many cities and towns lack any policy on how frequently they replace their equipment.
- **Documentation**. All security measures and policies should be adequately documented and disseminated to ensure that (1) the policies and procedures are understood and capable of being followed, (2) users understand the expectations

placed on them, and (3) when employee turnover occurs, critical information about information security is not lost.

- **Vulnerability assessments**. For organizations that can afford this extra step, a vulnerability assessment involves inventorying all systems, hardware, and software and assessing the points of vulnerability. A vulnerability report typically includes a list of recommended modifications. These assessments are usually performed every few years. Assessments can also include a "probe" element, where a deliberate attempt to gain unauthorized access to a system is made in order to educate users about vulnerabilities.

Municipalities Should Work Together for Increased Security

Forums for Information Sharing and Collaboration

The Grand Jury's investigation revealed that staff and elected officials in many Marin cities and towns are unaware that other jurisdictions in the county have been successfully attacked. Without this important information about breaches occurring among their peer group, city and town managers, as well as elected officials, are not alerted to the urgent need to reexamine their own security practices and to collaborate with their peers to improve the security of the entire group.

More transparency and better collaborative approaches could help Marin's smaller cities and towns become more sophisticated in their cybersecurity practices at a reasonable cost. Two existing groups that are well positioned to foster collaboration in this area are the Marin County Council of Mayors & Councilmembers (MCCMC) and the Marin Managers Association (MMA).

One stated purpose of MCCMC is to promote cooperation and collaboration among Marin's cities and towns "in the solution of mutual problems."[14] MCCMC has ad-hoc subcommittees devoted to such topics as disaster preparedness, homelessness, pension reform, and climate change, but they have no group devoted to cybersecurity. The Grand Jury's investigation revealed that MCCMC has not had a focus on helping cities, towns, or other agencies improve their cybersecurity practices. By making cybersecurity a priority and creating a public forum for discussion of the issue, MCCMC could promote greater cybersecurity awareness not only among mayors and councilmembers, but also among the public, local businesses, and nonprofit organizations.

MMA is composed of all of the town and city managers in the county, as well as the county administrator and the executive director of the Marin Municipal Water District. It serves as a forum for the managers not only to share their experiences and best practices for managing Marin's cities and towns, but also to exchange ideas about how they might share services to lower costs and improve efficiency. The Grand Jury's investigation revealed that MMA could do a better job of ensuring that experiences like the breaches described in this report are shared

[14] "About," Marin County Council of Mayors & Councilmembers, accessed April 15, 2020, http://www.mccmc.org/about/.

among its members, and that a higher priority is placed on cybersecurity in Marin's cities and towns.

Working in conjunction with the county's chief information security officer, MMA could assist the cities and towns in distilling the above suggestions regarding best practices to a specific list for implementation. In addition, the county's chief information security officer could start a special email list for city and town officials to keep them informed of cybersecurity alerts sent out by federal authorities, as well as provide regular email reminders to city and town staff to be prudent with external emails, attachments, and passwords. All of these efforts could be implemented at minimal cost.

Shared Services

Larger organizations can afford stronger security. For example, the county government has nearly 2,100 employees, more than 70 employees in its IT department, and a substantial IT budget. Marin's two largest cities, San Rafael and Novato, also have substantial IT budgets and devote significant resources to cybersecurity. On the other hand, several of Marin's smaller cities and towns do not have a full-time staff member devoted to IT management, using outside vendors instead.

Marin's cities and towns could turn to the Marin General Services Authority (MGSA) for assistance. MGSA is a joint powers authority formed for the purpose of administering shared programs among the county, cities, and towns.[15] With a shared program, each participant generally contributes a fixed amount per year for MGSA to manage the program. In turn, MGSA generally contracts with an independent consultant to deliver services to the participating jurisdictions.

For example, MGSA could establish a contract with an outside cybersecurity expert, who could then consult with individual cities and towns regarding their vulnerability and actions they could take to improve their security. Members could pay a base fee in exchange for a nominal service level, and then pay extra should they need more extensive consulting services. A shared cybersecurity program could be more effective than each city and town hiring its own consultant, because the MGSA consultant would acquire specific knowledge about the capabilities of the MIDAS wide area network and would not need to relearn those details on each assignment.

Beyond cybersecurity, MGSA might also explore the creation of shared IT procurement standards for cities and towns. For example, every city and town needs a financial management system for its budgeting, fund accounting, and human resources needs. If all the cities and towns were to standardize on the same third-party software, they would be in a much better position to negotiate for lower prices and to create cross-jurisdiction user groups to enhance all users' knowledge of how to use the system effectively. But if each city and town continues to act independently with regard to software selection and purchasing, efficiencies like this will not be possible.

[15] "History and Overview," Marin General Services Authority, accessed April 15, 2020, http://maringsa.org.

By moving toward a stronger culture of collaboration regarding IT needs, not just for cybersecurity, cities and towns would be able to enhance their performance while reducing their costs.

MIDAS Enhancements Could Improve Security

The county's MIDAS wide area network has provided a strong and secure backbone for Marin's municipalities for the past 25 years. With its firewalls and redundant, secure connection to the internet, it provides a good first line of defense against cyber criminals. However, as previously discussed, attacks that use fake emails as their entry point are not stopped by MIDAS, and MIDAS does not currently provide malware filtering or antivirus protection. In addition, the Grand Jury heard concerns that MIDAS is too costly and the internet speeds are too slow, which could result in some cities and towns deciding in the future to opt out of the system. This might weaken the security they currently enjoy.

Given the county's strong Information Services and Technology Department and its many years of experience with the MIDAS system, the county is well positioned to provide additional support and resources to Marin's cities and towns regarding cybersecurity.

In 2020, the county is performing a review of the MIDAS system for possible modifications, enhancements, and cost reduction. Modernizing and enhancing MIDAS could provide even more security, which would create a strong motivation for cities and towns to continue using the system or even rely on MIDAS more. Enhancements could include the following:

- Web filtering, where particular websites, especially those known to host malware, could be blocked automatically, or "blacklisted"
- Geo-blocking to block websites from certain countries or regions
- Email filtering to prevent known malware from getting through
- Real-time monitoring dashboards for better management capabilities
- Disaster recovery features

While these enhancements would undoubtedly come at some cost, it may be possible to make them elective for those cities and towns that believe the costs are justified.

Findings

F1. The Marin County government has a well-developed approach to cybersecurity in general, and a robust architecture and strategy for avoiding breaches.

F2. The Marin County government has substantial cybersecurity expertise and, as the host and manager of the MIDAS system, is well positioned to assist the cities and towns in developing a common set of best practices regarding cybersecurity.

F3. Transparency is lacking regarding cybersecurity because past breaches have not been publicly disclosed, and city and town councils have not facilitated public discussion of cybersecurity issues.

F4. Most elected officials in Marin's cities and towns are not sufficiently engaged in ensuring robust cybersecurity policies and procedures are in place.

F5. County and municipal officials and managers have been generally unaware of breaches that have occurred outside their own agencies in Marin and therefore have not felt the need to collaborate on measures to improve cybersecurity.

F6. Municipalities have been lax in following FBI guidance that cybersecurity breaches be reported to federal law enforcement.

F7. Marin's cities and towns have not made a concerted effort to standardize around a common set of best practices with respect to cybersecurity.

F8. The Marin County Council of Mayors & Councilmembers has not made cybersecurity a priority, which has minimized the awareness and engagement of elected officials in cybersecurity matters.

F9. The Marin Managers Association has not done enough to facilitate the sharing of cybersecurity information and resources among its members.

F10. Various low-cost best practices exist that could, if implemented, significantly improve the cybersecurity posture of Marin's cities and towns.

Recommendations

R1. Within 120 days of the date of this report, the Marin County Information Services and Technology Department should create an ongoing program to share user education information, other cybersecurity practices, and updates with cities and towns.

R2. Within 120 days of the date of this report, the Marin County Information Services and Technology Department should complete a plan for enhancing MIDAS to improve cybersecurity for its users.

R3. Within 120 days of the date of this report, the Marin County Information Services and Technology Department should offer to collaborate with the cities and towns, through the Marin Managers Association or another channel, to develop best practices for cybersecurity in Marin's cities and towns.

R4. Starting in fiscal year 2020–2021, the county board of supervisors and the city and town councils should request their managers report, at least annually, regarding their cybersecurity profile and any measures being taken to improve it.

R5. Starting in fiscal year 2020–2021, the county, cities, and towns should convene periodic discussions, at least annually, in a public forum such as a board or council meeting, regarding the importance of good cybersecurity practices for our government, residents, and other organizations.

R6. The county and each city and town should adopt a policy to report to federal law enforcement any cybersecurity intrusion that results in financial fraud or unauthorized disclosure of information and make that intrusion public.

R7. Within 180 days of the date of this report, cities and towns should implement the first four practices described in the Best Practices section of this report, regarding mandatory user training, email flagging and filtering, password management, and backup.

R8. In fiscal year 2020–2021, cities and towns should complete an analysis of the feasibility of implementing the remainder of the practices described in the Best Practices section of this report.

R9. In fiscal year 2020–2021, cities and towns should, through the Marin Managers Association, complete an analysis of the feasibility of contracting with a cybersecurity expert to be available to cities and towns on a shared basis, in order to raise the overall level of cybersecurity in Marin's cities and towns.

Request for Responses

According to the California Penal Code, agencies required to respond to Grand Jury reports generally have no more than 90 days to issue a response. It is not within the Grand Jury's power to waive or extend these deadlines, and to the Grand Jury's knowledge, the Judicial Council of California has not done so. But we recognize that the deadlines may be burdensome given current conditions caused by the COVID-19 pandemic.

Whether the deadlines are extended or not, it is our expectation that Marin's public agencies will eventually be able to return to normal operations and will respond to this report. In the meantime, however, public health and safety issues are of paramount importance and other matters might need to wait.

Pursuant to Penal Code Section 933.05, the Grand Jury requests responses from the following governing bodies:

- County of Marin (F1-F2, R1-R3)
- City of Belvedere (F3-F10, R4-R9)
- City of Larkspur (F3-F10, R4-R9)
- City of Mill Valley (F3-F10, R4-R9)
- City of Novato (F3-F10, R4-R9)
- City of San Rafael (F3-F10, R4-R9)
- City of Sausalito (F3-F10, R4-R9)
- Town of Corte Madera (F3-F10, R4-R9)
- Town of Fairfax (F3-F10, R4-R9)
- Town of Ross (F3-F10, R4-R9)
- Town of San Anselmo (F3-F10, R4-R9)
- Town of Tiburon (F3-F10, R4-R9)

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.

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.