COUNTY OF MARIN

DEPARTMENT OF INFORMATION SERVICES AND TECHNOLOGY

# Top 10 Cybersecurity Recommendations for Organizations 4/12/2022

## Introduction

Cyberattacks such as ransomware against government agencies, critical infrastructure, and businesses have become the norm. Cyber criminals launch attacks to disrupt operations, obtain unauthorized access to information, and extort money for their own financial gain.

While all organizations want to defend themselves from cyberattacks, they may not have the knowledge, expertise, or resources to know where to begin. What are the threats that they should be most concerned about? What protections do they already have in place? How can they identify and prioritize security improvements that they should implement?

To address these concerns, the County of Marin Department of Information Services and Technology in collaboration with the Marin Security and Privacy Council (MSPC) is providing a Top 10 list of cybersecurity recommendations for organizations.

## About the Top 10 List

The Top 10 List was created based on the County of Marin's direct experience in managing cybersecurity threats and responding to incidents. The list is not intended to be used as a cybersecurity framework or a comprehensive information security program. Organizations should evaluate and choose a cybersecurity framework based on their business needs and legal, regulatory,

and compliance requirements. Common cybersecurity frameworks include the CIS Critical Controls, NIST Cybersecurity Framework, and NIST 800-53.

The County of Marin also recommends that organizations follow cybersecurity guidance issued by the Cybersecurity & Infrastructure Security Agency of the Federal Government.

The Top 10 List provides recommendations to help organizations implement preventive, detective, and corrective security controls to mitigate the risk that a cyberattacks launched against them, particularly phishing and ransomware, will succeed. Organizations can use this list to conduct a gap analysis against their existing controls, systems, and processes to help them prioritize and implement security improvements.

**Top 10 List**

1. **Multi Factor Authentication (MFA)**
    - **Actions:** Implement and enforce Multi Factor Authentication (MFA) for critical applications, systems, and accounts, starting with access to organization e-mail for all employees. MFA requires an authentication in addition to a standard username and password combination and can be an effective tool in preventing unauthorized access to e-mail in the event a username and password are compromised.
    - **Risk Factors:** E-mail is one of the top targets of cyber criminals. If an attacker gains unauthorized access to an employee's mailbox, they can view the e-mail data including potentially sensitive information, use the e-mail address to launch additional phishing attacks both within and outside your organization, and set up rules to hide their tracks and have secret conversations with other members of your organization such as people in your finance and payroll departments.
    - **Recommendations:** While MFA enforcement on e-mail for all employees is priority #1, review all critical applications, systems, and

accounts that should also be addressed. Common areas include administrator accounts for both cloud and on-premises systems, Virtual Private Network (VPN) connections, and cloud productivity and collaboration platforms such as Office 365 and Google Workspace.

## 2. Cybersecurity Education, Awareness, and Training

- **Actions:** Implement mandatory cybersecurity awareness training for all employees, conducted at least annually. Implement e-mail mock phishing exercises to assess the effectiveness of your cybersecurity awareness training, conducted at least quarterly.
- **Risk Factors:** While technical security controls can reduce the number of phishing e-mails that get through your organizations' defenses, inevitably some will get through and land in the Inboxes of your employees. Most successful e-mail phishing attacks rely on the recipient to click a link, open an attachment, and/or provide a username or password. Educating your employees on cybersecurity best practices for e-mail, passwords, web browsing, social media, mobile devices, and more will improve your chances that they will take appropriate actions to protect your organization rather than falling for the phish.
- **Recommendations:** Offer cybersecurity trainings in multiple subjects that can be taken in short increments of 5-15 minutes, with the total amount of training each year adding up to at least one hour. Assess the results of e-mail mock phishing exercises against industry benchmarks for your sector and conduct follow-up trainings with "frequent clickers" as needed. Reinforce cybersecurity tips and best practices through regular communications such as the County's monthly cybersecurity awareness newsletter. Encourage employees to participate in the County's annual cybersecurity events during October Cybersecurity Awareness Month.

3. **Endpoint Security**
    - **Actions:** Implement an Endpoint Detection and Response (EDR) solution to all clients and servers managed by the organization. Implement a whole-disk encryption solution on all endpoints.
    - **Risk Factors:** Traditional signature-based antivirus solutions are incapable of detecting, preventing, and containing modern malware attacks such as ransomware. A single compromised endpoint can infect additional clients and servers, putting your entire organization at risk of system downtime, data loss, data breach, and financial loss.
    - **Recommendations:** Implement an EDR solution that supports all hardware and software platforms used by your organization and has behavioral monitoring capability in addition to relying on known malware signature databases. Modern EDR solutions provide enhanced visibility into system activities, simplify incident response activities, and allow organizations to isolate known-infected endpoints as needed. Implement a whole-disk encryption solution on all endpoints to protect organizational data in the event an asset is lost or stolen.

4. **E-mail Security Hardening**
    - **Actions:** Implement Domain-based Message Authentication (DMARC), Domain Keys Identified Mail (DKIM), and Sender Policy Framework (SPF) for all organization e-mail domains. Implement anti-virus, anti-spam, anti-phishing, and policy-based rules to minimize malicious e-mails and protect sensitive data. If you are a California government agency, migrate from your existing domain name to a .CA.gov domain name.
    - **Risk Factors:** DMARC, DKIM, and SPF combined add authentication, policy, reporting, and digital signatures to e-mail messages. E-mail domains that do not have DMARC, DKIM, and SPF configured are at increased risk of spoofing attacks. E-mail domains that do not filter for malware, spam, and phishing messages are at increased risk of

malicious attacks. When domains are unprotected, cyber criminals can send e-mails using the organization's domain, infect systems with malware, steal employee credentials, and launch attacks that may lead to system downtime, data loss, security breaches, and reputational harm.

- **Recommendations:** Implement DMARC, DKIM, and SPF to protect e-mail domains from spoofing attacks. Perform the initial implementation in passive / monitoring mode to determine configuration changes that may be required for sending e-mails via authorized 3rd party provider. Change the configuration to active/enforcement mode when you are confident you have addressed the requirements. In addition to standard antivirus and antispam tools, implement policies to detect and block or encrypt outgoing e-mails that contain Personally Identifiable Information (PII) or Protected Health Information (PHI) such as date of birth, social security number, and driver's license number. For government agencies, .CA.gov domain names provide enhanced security and assurances to the public that they are communicating with legitimate government agencies.

## 5. Vulnerability Management

- **Actions:** Implement tools and processes to identify and remediate vulnerabilities as they are discovered, for both on-premises and remote systems.
- **Risk Factors:** New vulnerabilities are constantly being discovered for operating systems and 3rd-party software. Vendors typically release updates at least monthly, and in some cases more frequently if zero-day vulnerabilities are discovered. Currently supported systems that go unpatched and legacy systems that no longer receive security updates are frequently targeted by cyber criminals. With many employees working from home, existing patch

management tools may not be able to communicate with remote endpoints.

- **Recommendations:** Implement patch management tools that are capable of identifying and remediating vulnerabilities for operating systems and authorized 3rd-party software. Only use currently supported operating systems and software. Ensure that the tools can manage all servers and endpoints, including ones that are primarily used remotely. Implement processes that ensure all systems are patched regularly. Patches should be applied within 14 days of release, with critical patches being applied as soon as possible. For zero-day vulnerabilities, prioritize public-facing systems and the highest value assets first.

## 6. Password Policy and Management

- **Actions:** Implement a password policy in alignment with the National Institute of Standard and Technology (NIST) Special Publication 800-63B recommendations. Implement password management tools to help employees securely manage multiple accounts and passwords.
- **Risk Factors:** Compromised passwords are a common entry point for cyber criminals. A poorly chosen password may result in unauthorized access to an organization's systems and data, and provider attackers with an entry point to install malicious software such as ransomware. Employees that use weak passwords or the same passwords for all their accounts put the organization at increased risk of compromise.
- **Recommendations:** Implement a password policy that favors length over complexity, encouraging employees to use long passphrases (14 characters or more) in lieu of passwords. Implement MFA whenever possible. Ensure employees do not reuse the same passwords for multiple accounts and understand that if they suspect an account has been compromised their passwords

need to be changed immediately. Consider implementing a password management tool for employees to secure multiple accounts and passwords.

7. **Phish Reporting Workflow**
    - **Actions:** Implement processes and tools to manage the reporting, analysis, and remediation of potential phishing e-mails.
    - **Risk Factors:** Cybersecurity training materials educate employees about potential threats and how to identify them. If there is no clear process for phish reporting in place employees may not know what to do if they receive a phishing e-mail. Do they forward the e-mail to their supervisor or IT support? Do they delete the e-mail? If they do nothing, what happens to other employees who received the same e-mail? Absent process, employees may take actions that may place the organization at increased risk.
    - **Recommendations:** Implement a process for employees to report suspected phishing e-mails to the IT support team responsible for cybersecurity. Depending on the anticipated volume of e-mails reported and IT resource constraints, consider integrating the phish reporting process with your ticketing system and/or implementing tools to support the analysis, remediation, and eradication of actual phishing e-mails.

8. **Security Incident Response**
    - **Actions:** Implement security incident response procedures in alignment with the National Institute of Standard and Technology (NIST) Special Publication 800-61 recommendations.
    - **Risk Factors:** In the event of a suspected or actual security incident, it is important to have incident response procedures prepared in advance. Without incident response procedures in place, several issues can occur such as delays in recovery, additional assets

becoming compromised, and a lack of communication and coordination among the people responding to the incident. Any issues in response efforts can put an organization at increased risk. A lack of visibility into user, network, and system activities can

- **Recommendations:** Implement security incident response procedures that address each of the phases of the incident lifecycle: 1. Preparation, 2. Detection and Analysis, 3. Containment, Eradication, and Recovery, 4. Post-Incident Activity. Leverage the Cybersecurity Response and Recovery Planning frameworks and toolkits developed by the Bay Area Urban Areas Security Initiative (UASI) to organize your plans. Develop an incident response plan specific to recovery from ransomware attacks. Conduct tabletop exercises and update plans at least annually.

**9. Secure Backup Infrastructure**

- **Actions:** Implement a secure backup infrastructure to protect the organization's critical systems and data from malicious attacks such as ransomware.
- **Risk Factors:** A solid backup infrastructure is critical to recover from outages. Cyber criminals target both live systems and data backups with ransomware to hold systems hostage. If system backups are compromised, organizations have no choice but to pay the ransom or accept data loss.
- **Recommendations:** Implement a backup infrastructure that is isolated from primary systems and includes multiple copies of backups. Ensure there is at least one set of backups that cannot be accessed from the organization's network. Consider investing in fast storage solutions with solid state drives for backup infrastructure to recover more quickly. Test restoration from backups at least annually.

## 10. Cloud and Network Security

- **Actions:** Implement access controls for cloud and on-premises systems to reduce the organization's attack surface. Implement proper network segmentation between trusted and untrusted devices and zones. Implement tools to provide visibility into user, network, and system activities and alert on suspicious activities and anomalies.
- **Risk Factors:** Default configurations may allow connectivity to cloud and on-premises resources from any device, anywhere, and at any time. Systems and networks that are not hardened to limit access based on least privilege are more susceptible to malicious attacks. If your organization lacks visibility into potentially suspicious activities, cyber criminals may gain access to your network and create persistent connections without your knowledge.
- **Recommendations:** Implement Geo-blocking for cloud and on-premises systems to restrict connectivity to your organization's resources from authorized locations only. Leverage threat feeds to automatically block known malicious domains and IP addresses. Only open ports and services as required for systems and applications to function, especially with public-facing systems. Segment your networks to restrict access based on security requirements, taking extra care to segment Internet of Things (IoT) devices, building management systems, and guest Wi-Fi networks. Use the concept of least privilege when assigning permissions to devices and network resources. Monitor your systems and networks for signs of suspicious activity such as concurrent connections from the same employee from multiple devices and/or locations.

**Disclaimer**

The information provided by the County of Marin in this document is intended to increase an organization's awareness of cybersecurity threats and provide recommendations to help them improve their organization's cybersecurity posture and defenses. All information in this document is provided in good faith, however the County of Marin makes no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information in this document.

Links in this document are provided because they have information that may be useful. The County of Marin does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of County of Marin.

Under no circumstance shall the County of Marin have any liability to you for any loss or damage of any kind incurred resulting from the use of this document or reliance on any information provided within it. Your use of this document and your reliance on any information contained within is solely at your own risk.