LEAGUE OF CALIFORNIA CITIES

Recovering From Ransomware

Donald Hester
Director of IT Audit, Maze & Associates
Benjamin Buecher
IT Manager City of Lodi
Doug Alessio
Administrative Services Director, City of Livermore

Agenda

- Ransomware the current situation
- Lessons Learned
- What went right
- What went wrong
- What we are doing now
- What you should do now

The Current Situation

LEAGUE OF CALIFORNIA CITIES

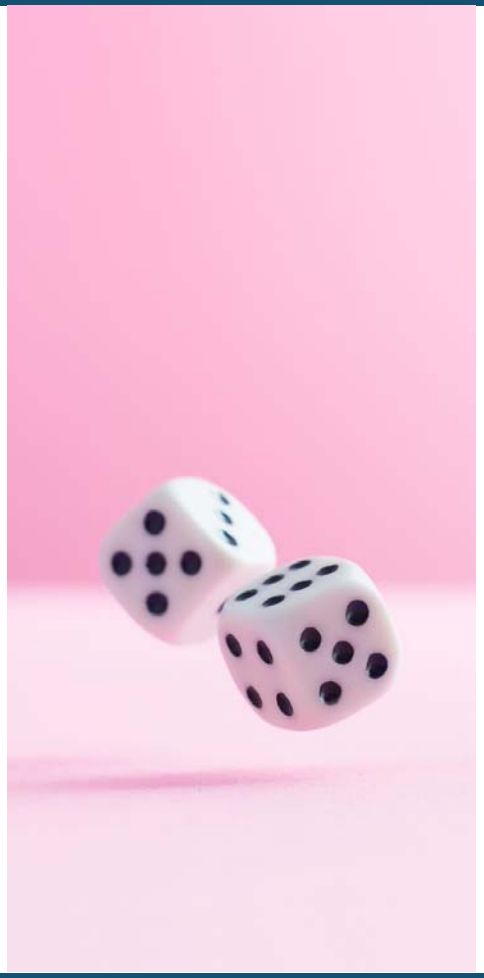
What do you think is the likelihood that your organization is a target?

The Current Situation

- Disaster recovery plan? What plan?
- Talent Gap in Cybersecurity
- Spend on average 2% of IT budget on cybersecurity (GFOA)
- COVID-19 Pandemic – Remote Workforce
- Revenue short fall – Spending cuts across all departments
- Asking too much from IT staff
- The need to prioritize cybersecurity during budget cuts
- Continue to be a target for cyber-criminals – ransomware
- Ransoms are going up
- Cyber criminals releasing data if ransom is not paid

Potential Impact

- 2020 a perfect storm
- Not “If” but “When”
- Pay Now or Pay More Later
- Total disruption of City business
- Impact Beyond Downtime
- Bond Rating
- Insurance Costs
- This is not an “IT” problem
- Cyber risk is **business risk**



LEAGUE OF CALIFORNIA CITIES

Cyber Incidents Ranked as No. 1 Business Risk

Cyber incidents are now the No. 1 business risk facing corporations, moving to the top of insurer Allianz's annual list, which also showed climate change reaching its highest ranking.

According to the **Allianz Risk Barometer for 2020**, 39 percent of respondents to its ninth annual survey of risk experts identified cyber incidents as their main concern, pushing business interruption events (37 percent) out of the top spot it had occupied for seven years.

The survey also showed climate change moving up to the No. 7 ranking (17 percent of responses), joining changes in regulation and legislation (No. 3 with 27 percent of responses) as the biggest climbers.

In the U.S., cyber risk took the top spot followed by business interruption and natural catastrophes. Allianz noted that a mega data breach, involving more than one million compromised records, now costs on average $42 million, up 8 percent year on year.

blogs.calcpa.org/hot-topics/calcpa-buzz-thank-successful-cpa-day/

LEAGUE OF CALIFORNIA CITIES

How long can your organization effectively and efficiently operate without technology or data?

LEAGUE OF CALIFORNIA CITIES

The Federal Government recommends immediate action to safeguard against ransomware attacks.

Lessons Learned

What is the biggest lesson learned from being a ransomware victim?

What Went Right?

Was there a silver lining?

What did staff do right to limit the impact or to reduce the recovery time?

What Went Wrong?

What would you do you wish you could have done differently?

LEAGUE OF CALIFORNIA CITIES

What we are doing now?

Now that you have recovered what is changing?

What are you doing to limit the possibility of cyber incidents?

What are you doing to limit the impact of cyber incidents?

What you should do now?

Prevention

1. Implement Governance of Information and Technology
2. GAP analysis of current controls
3. Prioritize control implementation

Governance

- Enterprise Governance of Information and Technology (EGIT) is concerned with value delivery from digital transformation and the mitigation of business risk that results from digital transformation.

https://www.isaca.org/Pages/Glossary.aspx

Governance of I & T

CIO

Information Technology

Information Systems

Service and value

CISO

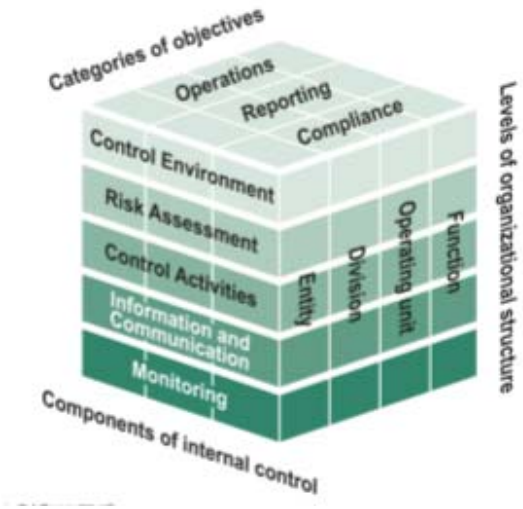
Cybersecurity

Risk & Compliance

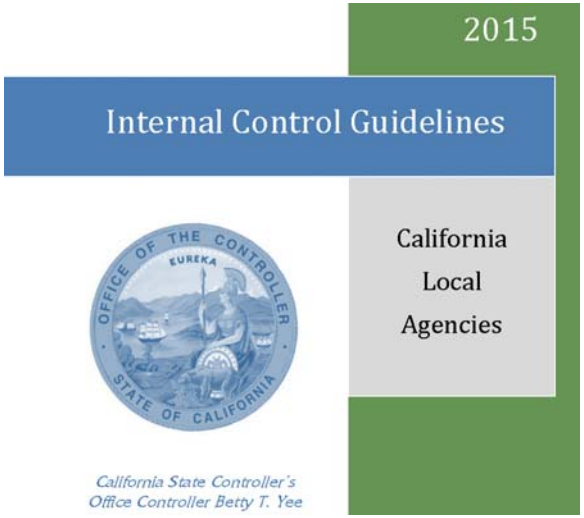
Safety and security

Governance and Internal Controls

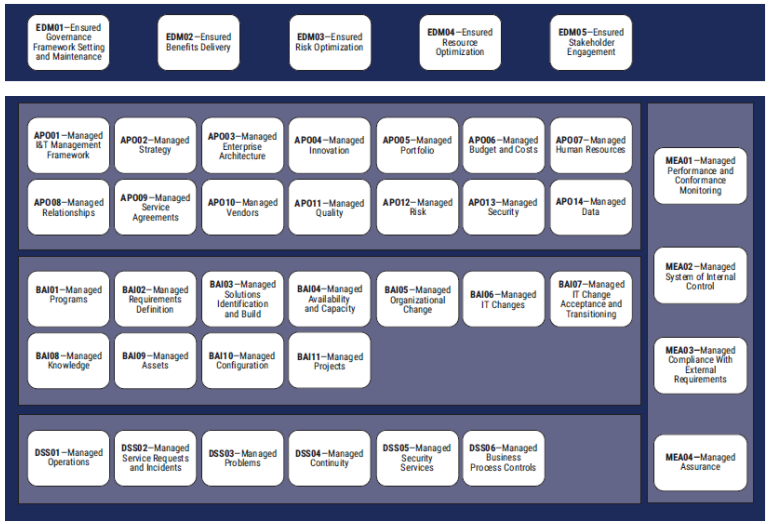
It's all about the mission



COSO Framework



Internal Control Guidelines



COBIT 2019

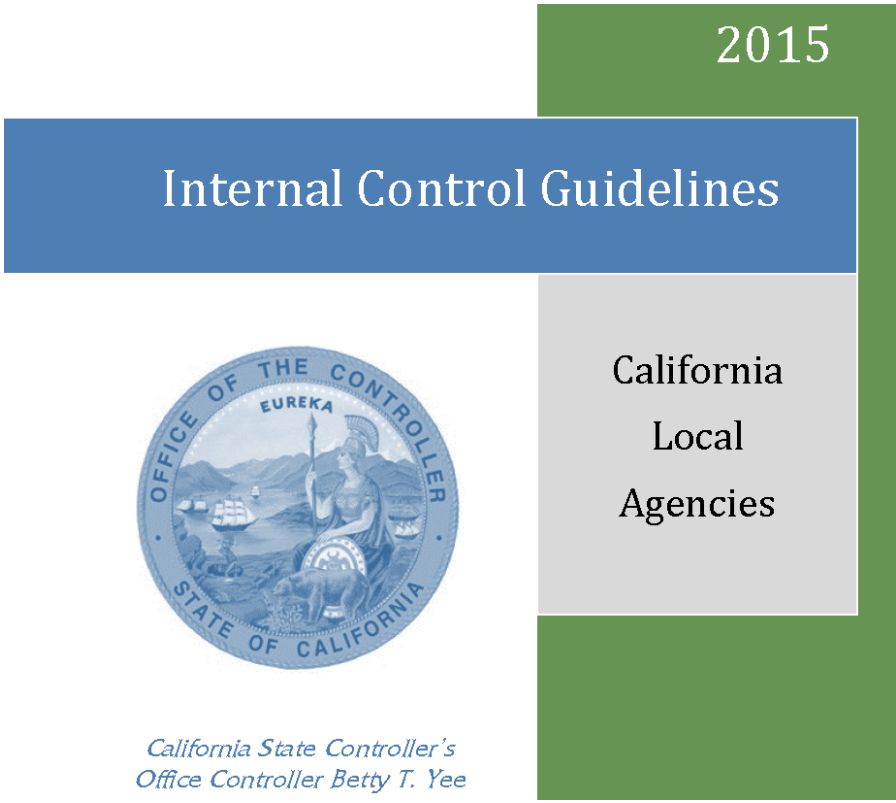
Internal Controls

Cyber Risk Management

"The Information Technology (IT) department should periodically identify and communicate risks for which employees should be particularly vigilant."

"Application Controls and General IT Controls, which relate to the overall effectiveness of IT controls to ensure the proper operation of the local government's information systems."

Follow Industry Standards



https://www.sco.ca.gov/Files-AUD/2015_internal_control_guidelines.pdf

NIST Cybersecurity Framework (CSF)

- This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk.
- The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

LEAGUE OF CALIFORNIA CITIES

What are you going to change when you get back to the office?

LEAGUE OF CALIFORNIA CITIES

"The way to get started is to quit talking and begin doing."

- Walt Disney

LEAGUE OF CALIFORNIA CITIES

Appendix

Use this checklist to perform a GAP analysis to determine what controls need to be put in place.

Checklist - Planning

- Briefing for senior management on the risk to mission and business operations.
- Senior management should discuss if paying a ransom is an option, should an attack happen.
- Consider purchasing cyber insurance to cover the costs of recovery.
- Evaluate the current cyber insurance to see if the coverage is adequate to cover the cost of an extended recovery.
- Evaluate the current cyber insurance to ensure any exclusions exist that may limit what can be done in a ransomware event.
- Participate in cybersecurity information sharing programs such as InfraGard or MS-ISAC.

Checklist – Prevent & Limit

- Setup a cybersecurity awareness and training program for all staff.
- Create a comprehensive inventory that includes all software, services, devices, and cloud service providers.
- Assess the risk of third-party access to your systems.
- Create a formal incident response plan.
- Ensure the incident response plan is available offline.
- Review your incident response plan annually.
- Test your incident response plan annually.
- Update your incident response plan to include a containment strategy to isolate infect systems once discovered.
- Update your incident response plan to include steps to ensure backup are not connected to the contaminated network.
- Update your incident response plan to include contacting external resources such as the regional fusion center, antimalware vendor, and insurance carrier.
- Update your incident response plan to include steps to collect evidence including portions of the encrypted data.

Checklist – Prevent & Limit (cont.)

- Update your incident response plan to include steps to change all online and network passwords.
- Update your incident response plan to include steps to include steps to ensure a complete eradication of the malware and deleting any corrupted register keys.
- Update your incident response plan to include steps to include after action steps to determine root cause and determine future preventative measures
- Update your incident response plan to include steps to determine if decryption keys are freely available.
- Remind users regularly to promptly report any incidents.
- Consider having alternative communications planned assuming email and phones are not available.
- Consider adding advanced threat protection mechanisms to your email service.
- Add anti-phishing protections to email.

Checklist – Prevent & Limit (cont.)

- Add anti-spoofing mechanisms to email service.
- Consider a warning banner on all external emails.
- Configure your firewall to block all know malicious domains and IP addresses.
- Develop a centralized patch management process that includes all devices included firmware, software, operating systems and IoT devices.
- Apply vender patches within 30 days of release.
- Install anti-malware on all systems that support it.
- Update anti-malware as close to real time and possible.
- Setup all privileged accounts (admin or root) with the least privilege needed.
- Setup all privileged accounts (admin or root) with Multi-factor Authentication (MFA).
- Restrict users' permissions to run and install software applications using the "least privilege" principle.

Checklist – Prevent & Limit (cont.)

- Restrict permissions for system and service accounts on all systems.
- Limit user account access to the least access necessary to perform their job function.
- Setup application whitelisting and Software Restriction Policies.
- Develop a data classification scheme.
- Consider disabled Remote Desktop Protocol (RDP) or using VPNs for remoted desktop connections.
- Secure internal network Remote Desktop Protocol (RDP) connections.
- Disabled SMBv1 on all systems.
- Limit the use of SMB shares and audit access.
- Limit SMB communication to between servers and endpoints.
- Conducted annual penetration tests.
- Perform internal and external vulnerability scans at least monthly.

Checklist – Prevent & Limit (cont.)

- Address the vulnerabilities in a timely manner.
- Implement a mature change management process.
- Develop configuration baselines for all systems.
- Remove all obsolete, outdated, or unsupported devices, applications, and operating systems from your network.
- Segment your network to limit lateral movement across the enterprise network.
- Restrict Internet access for systems an users from harmful sites, especially known malicious sites

Checklist - Detect

- Run regular anti-malware scans regularly.
- Ensure ransomware prevention and detection is configured in the anti-malware software.
- Turn on audit logs for changes to privileged accounts.
- Monitor for changes to configuration baselines.
- Implement file integrity monitoring.

Checklist - Recover

- Develop an IT Business Continuity Plan.
- Preform a Business Impact Analysis to determine a prioritized recovery.
- Validated recovery goals with key stakeholders and executive management.
- Perform an annual review of the Business Continuity Plan.
- Ensure the business continuity plan available offline.
- Review backup schedules to determine if they align with business priorities.
- Ensure backups include systems, configurations files and data.
- Verify and test backups to determine if they can be recovered.
- Store backups so that they are not permanently connected to the network.
- Run exercises and testing of your business continuity plan annually.