TECH SAVVY, HR WISE & FISCALLY READY

Standardizing for Success

Update the JPA Standards to combat the current threat landscape

CAJPA
California Association of Joint Powers Authorities

George Reynolds

Chief Information Officer

CSAC Excess Insurance Authority

And

Carl Sandstrom

Business Projects Manager

California Joint Powers Insurance Authority

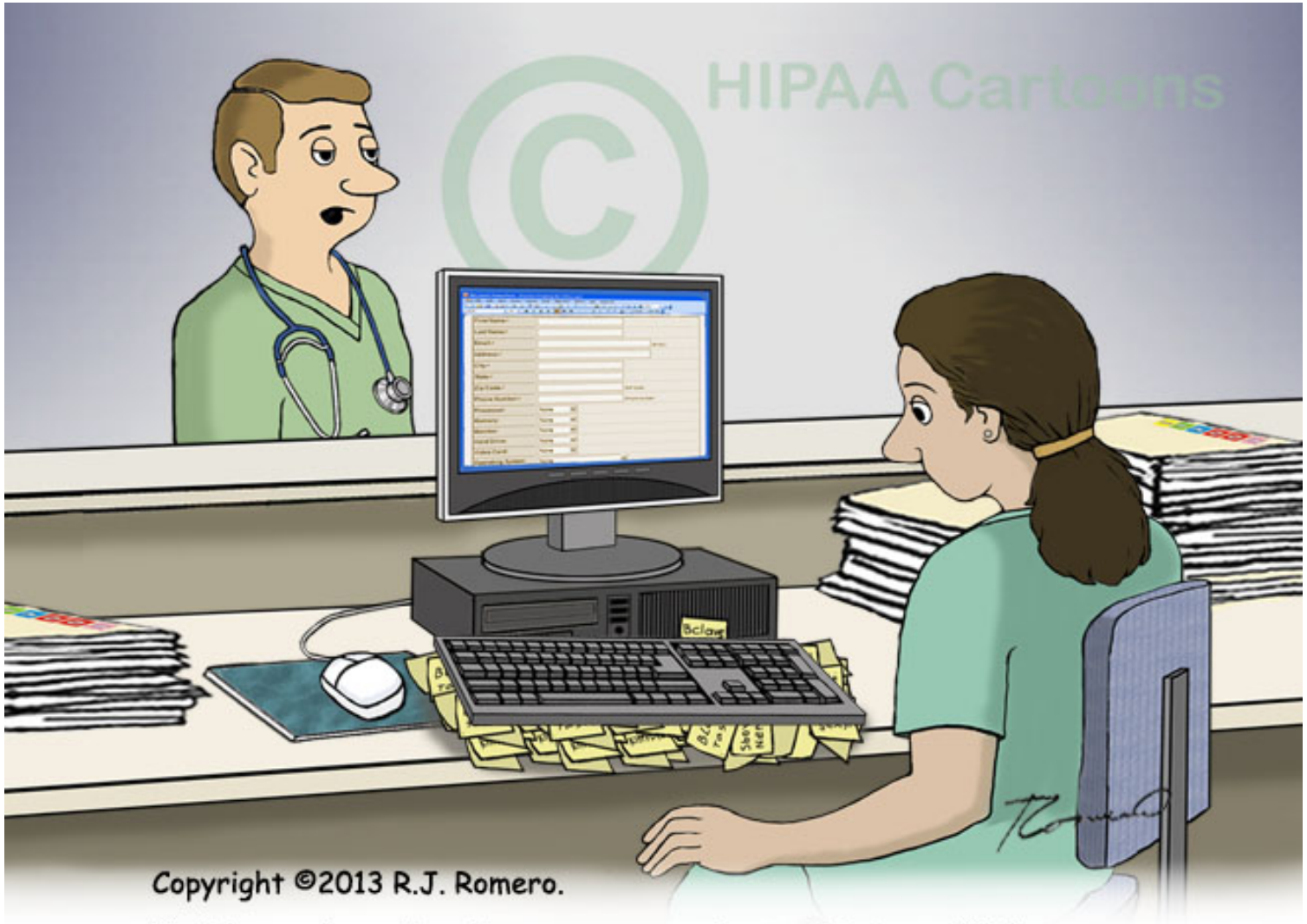
Standardizing for Success – Update the JPA Standards to combat the current threat landscape

Overview of Agenda:

- Why have IT Policies?
- Are we the only one doing this?
- Why update the CAJPA Accreditation Standards?
- What is going on and how do we protect ourselves?
- A Simple 5 Step Approach to IT Security
- What is the Current CAJPA Accreditation Standard?
- What needs to be added?

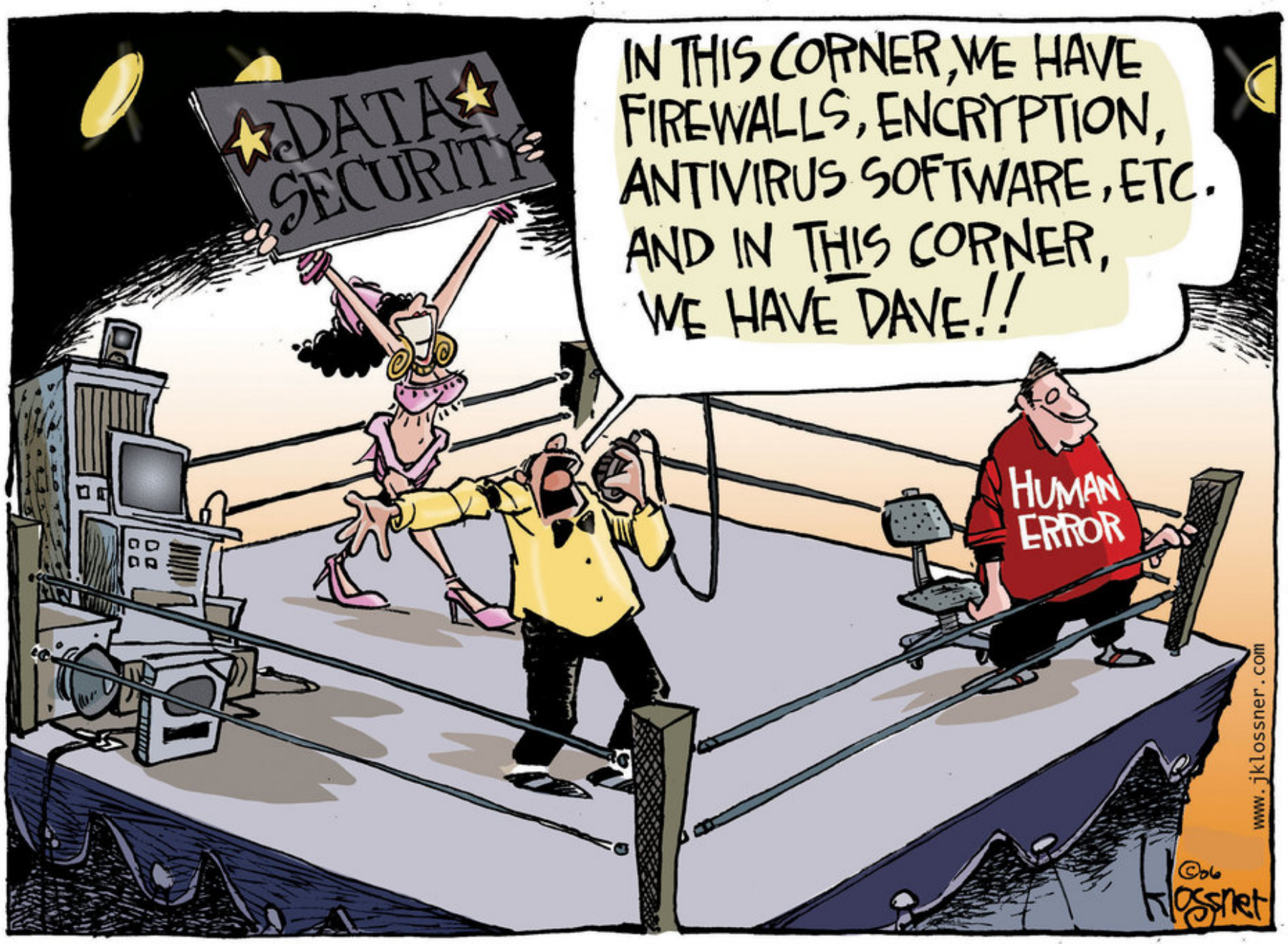
CAJPA
California Association of Joint Powers Authorities

Why have IT Policies?

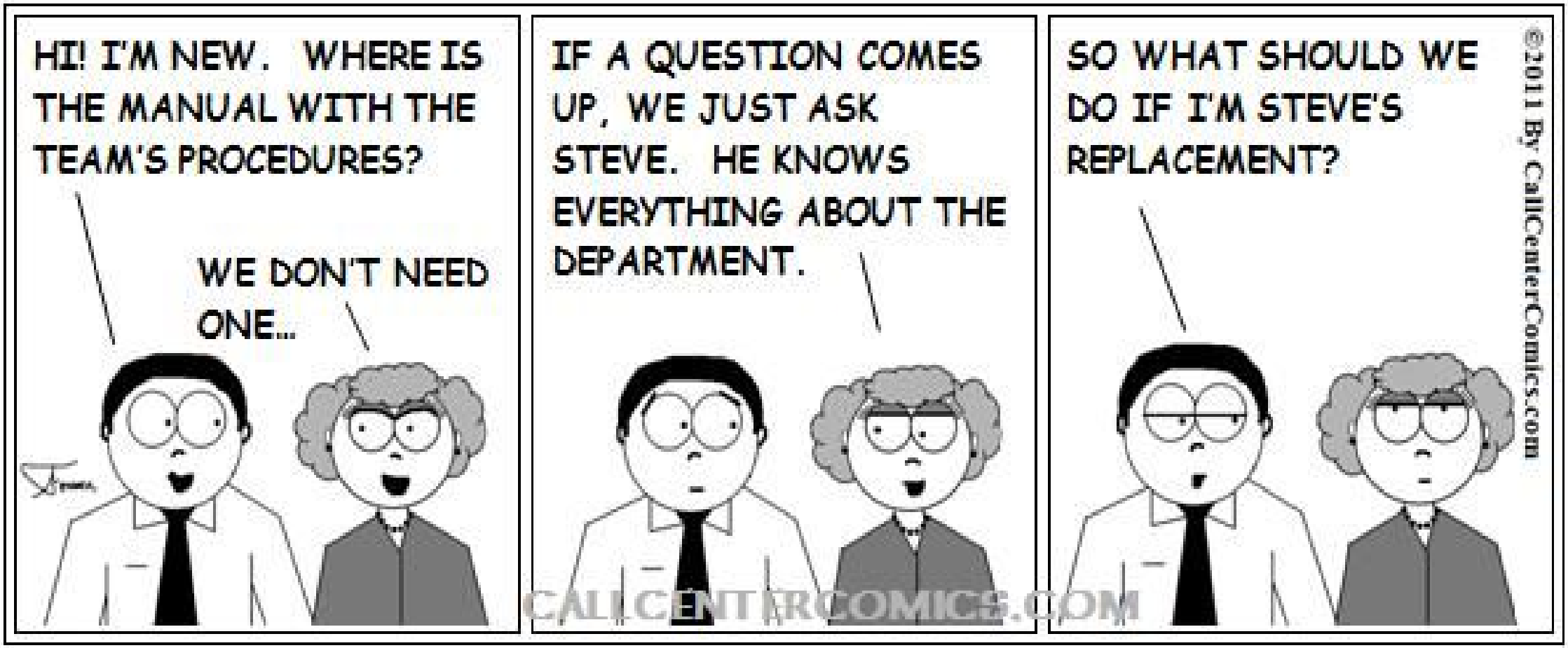


"Oh, that's for security. We all keep our user name and password on a sticky note hidden where it's safe."

CAJPA
California Association of Joint Powers Authorities



CAJPA
California Association of Joint Powers Authorities



CAJPA
California Association of Joint Powers Authorities

Why have IT Policies?

- Provide direction to staff
- Support your goal of providing services (Everyone knows how to do IT better than you)
- Support goal of implementing best practices (Cheap, Fast, and Secure – Pick two)
- Newer Insurance Policies (like Cyber Insurance) are requiring it
  - Additionally those insurance companies expect that we are following those IT Policies

Are we the only one doing this?

- We are not alone:
  - CCISDA – California County Information Services Directors Association
    - California Counties IT Policies for the Countywide Information Security Program
    - Created in 2002, updated in 2016 (152 pages)
  - MISAC – Municipal Information Systems Association of California
    - Excellence in IT Practice Award
  - State of California – California Office of Information Security
    - Information Security Risk Assessment Checklist
    - Nov 2009
  - Schools - ?

Why update the CAJPA Accreditation Standards?

- Last update was in 2008
- Rise of Data Incidents (Incidents, Breaches, and Ransomware)
- Speed at which the world has changed and is changing

CAJPA
California Association of Joint Powers Authorities

What is going on and how do we protect ourselves?

Old thinking: Focus on the top 5 CIS Controls and you will be covered

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges

What is going on and how do we protect ourselves?

Top 11 attack vectors

1) Phishing
2) Social Engineering
3) Ransomware
4) Downloaders
5) Drive-by Downloads
6) Malvertising
7) Zero-day attack
8) Password Cracking
9) Distributed Denial of Service Attack
10) Scareware
11) SQL Injection

A Simple 5 Step Approach to IT Security

1) Focus on what matters
2) Proactively assess your cyber risk
3) Build a multilayered defense
4) Fortify your organization
5) Prepare for the inevitable

CAJPA
California Association of Joint Powers Authorities

A Simple 5 Step Approach to IT Security

1) Focus on what matters

- Know what you have (asset management), know what is normal
  - Cradle to grave procedures for acquiring to disposing of equipment
  - Hardening systems
- Access control
  - Change default settings
  - Limit access to administrative privileges
  - Password management
    - Change passwords
    - Strong passwords
    - Don’t repeat passwords

A Simple 5 Step Approach to IT Security

2) Proactively assess your cyber risk

- Vulnerability assessment
- Monitoring
- Patch management – update software, rigorous patching schedule

A Simple 5 Step Approach to IT Security

3) Build a multilayered defense

- Protect the perimeter
- Anti-virus, anti-malware, spam protection, data encryption, web filter, website security
- Work and personal devices separate
- Manage the connectivity

A Simple 5 Step Approach to IT Security

4) Fortify your organization

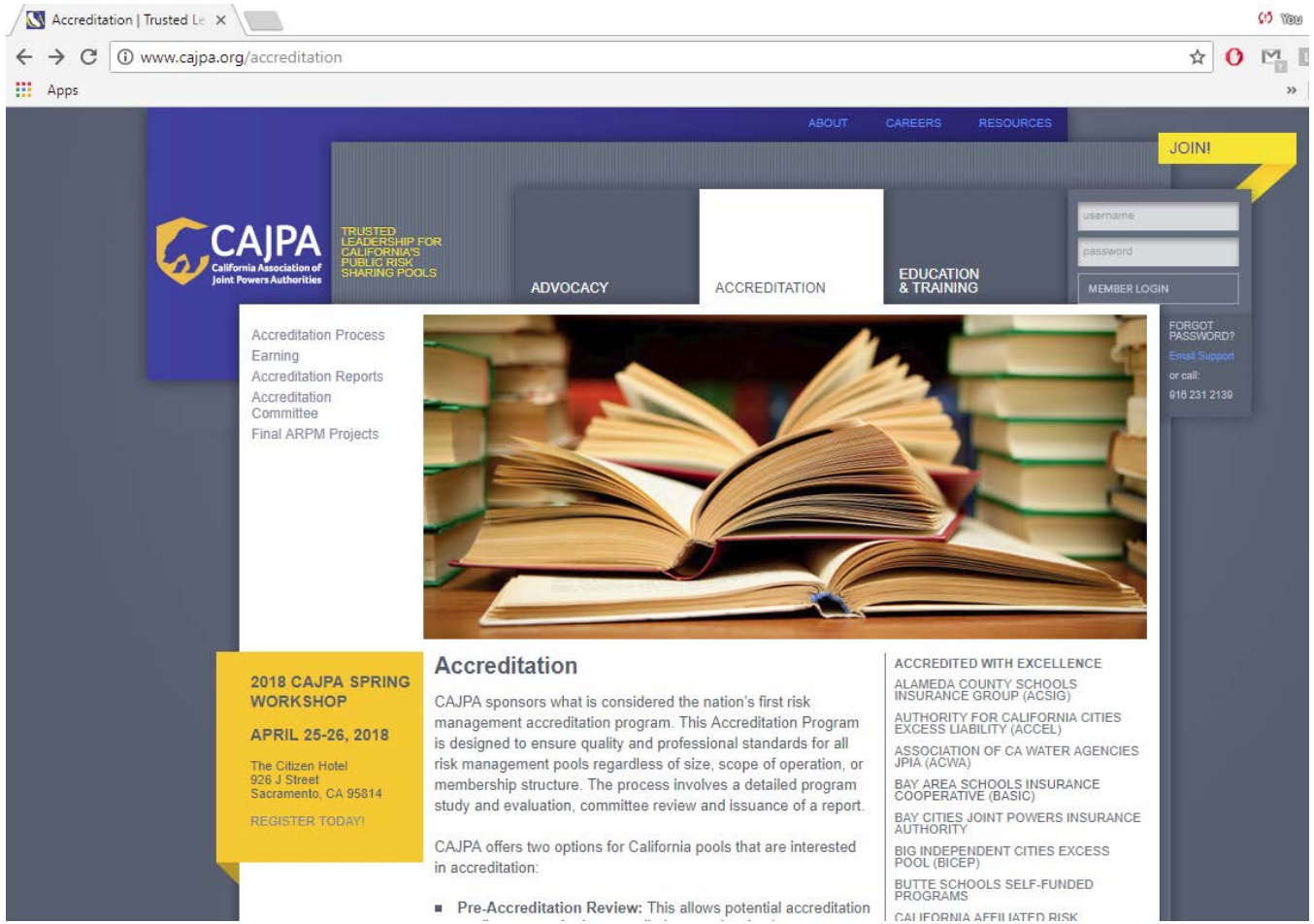
- Awareness and Training – Every body is responsible for security
- Confirm your vendor's security

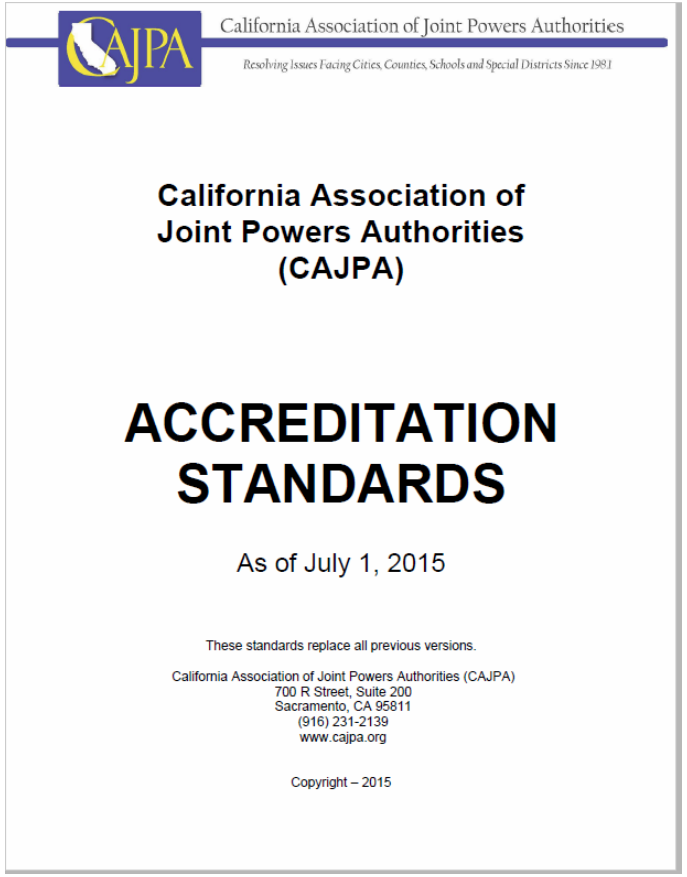
A Simple 5 Step Approach to IT Security

5) Prepare for the inevitable

- Ransomware
- Incident Response (Incident and Breach)
- Backup/Restore
- Disaster Recovery Plan
- Business Continuity Plan

What is the Current CAJPA Standard?

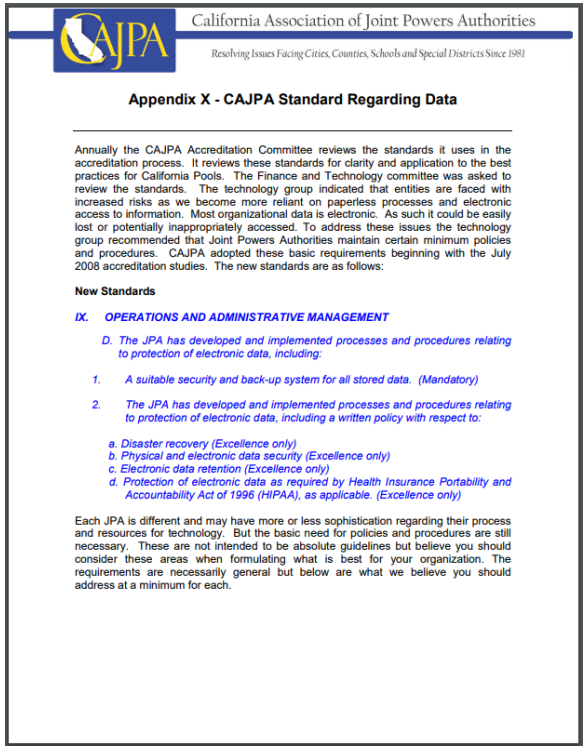




Standardizing for Success – Update the JPA Standards to combat the current threat landscape

CAJPA
California Association of Joint Powers Authorities

What is the Current CAJPA Standard (2015 Accreditation Standards – Appendix X)?



California Association of Joint Powers Authorities

Resolving Issues Facing Cities, Counties, Schools and Special Districts Since 1981

Appendix X - CAJPA Standard Regarding Data

Annually the CAJPA Accreditation Committee reviews the standards it uses in the accreditation process. It reviews these standards for clarity and application to the best practices for California Pools. The Finance and Technology committee was asked to review the standards. The technology group indicated that entities are faced with increased risks as we become more reliant on paperless processes and electronic access to information. Most organizational data is electronic. As such it could be easily lost or potentially inappropriately accessed. To address these issues the technology group recommended that Joint Powers Authorities maintain certain minimum policies and procedures. CAJPA adopted these basic requirements beginning with the July 2008 accreditation studies. The new standards are as follows:

New Standards

IX. OPERATIONS AND ADMINISTRATIVE MANAGEMENT

D. The JPA has developed and implemented processes and procedures relating to protection of electronic data, including:

1. A suitable security and back-up system for all stored data. (Mandatory)

2. The JPA has developed and implemented processes and procedures relating to protection of electronic data, including a written policy with respect to:

a. Disaster recovery (Excellence only)
b. Physical and electronic data security (Excellence only)
c. Electronic data retention (Excellence only)
d. Protection of electronic data as required by Health Insurance Portability and Accountability Act of 1996 (HIPAA), as applicable. (Excellence only)

Each JPA is different and may have more or less sophistication regarding their process and resources for technology. But the basic need for policies and procedures are still necessary. These are not intended to be absolute guidelines but believe you should consider these areas when formulating what is best for your organization. The requirements are necessarily general but below are what we believe you should address at a minimum for each.

JPA has developed and implemented processes and procedures relating to protection of electronic data, including:

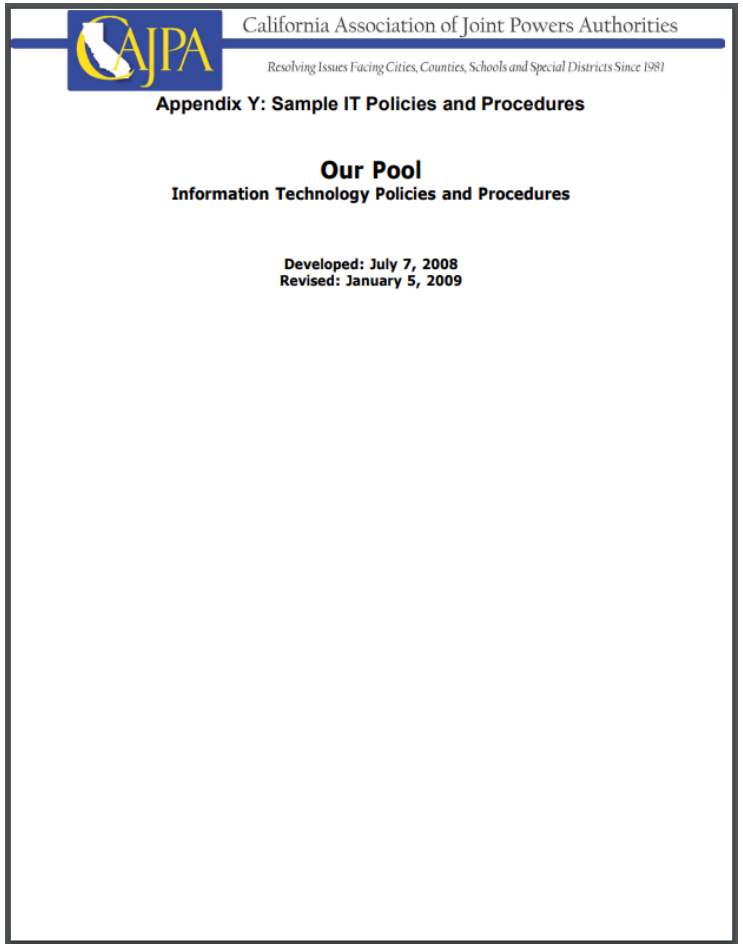
1. A suitable security and back-up system for all stored data.
2. A written policy with respect to:
    a. Disaster recovery (Excellence only)
    b. Data backup retention and recovery (Excellence only)
    c. Physical and electronic data security (Excellence only)
    d. Electronic data retention (Excellence only)
    e. Protection of electronic data as required by Health Insurance
    f. Portability and Accountability Act of 1996 (HIPAA), as applicable. (Excellence only)

CAJPA
California Association of Joint Powers Authorities

CAJPA Accreditation Standard:

Appendix Y: Sample IT Policies and Procedures

- Acceptable Use
- Security/Privacy
- Disaster Planning
- Backup and Recovery
- Email and Messaging
- Appropriate Use
- Remote Computing
- E-Data Retention
- Telephone and Cellular devices
- Internet Usage


California Association of Joint Powers Authorities

Resolving Issues Facing Cities, Counties, Schools and Special Districts Since 1981

Appendix Y: Sample IT Policies and Procedures

Our Pool

Information Technology Policies and Procedures

Developed: July 7, 2008
Revised: January 5, 2009

CAJPA
California Association of Joint Powers Authorities

What needs to be added to the CAJPA Standard?

- Security Awareness
- Incident Response
  - Including Data Breach Management
- Vendor Access/ Vendor Security Policies
- Remote Access
- Audit of Security Program – Security Assessment
- Vulnerability Assessment/Penetration Testing
- Automated patch management, anti-virus signature updates, network monitoring

Standardizing for Success – Update the JPA Standards to combat the current threat landscape

CAJPA
California Association of Joint Powers Authorities

TECH SAVVY, HR WISE & FISCALLY READY

Thank You!

CAJPA
California Association of Joint Powers Authorities