Information Security Officer

✓ IT Manager, Technical Support (Infrastructure)

- Desktop Support
- Telecommunications (Telephone System)
- Server Administration
- Networking / Security

Information Security Officer

- ✓ Appointed El Dorado County Information Security Officer, 2006
- ✓ Memberships and Affiliations
  - ▪ FBI Infragard, Computer Security Institute (CSI), CCISDA ISF, CA Office of Information Security
- ✓ Education
  - GIAC Security Essentials Certification (GSEC)
  - Certified Information Security Manager (CISM) Certification
  - Certified Information Systems Security Professional (CISSP) (in process), attended a three month training curriculum
  - Manage all security appliances and devices currently for El Dorado County
  - Chair the ITSSC (IT Coordinators and IT Analysts throughout EDC)
  - Master’s Degree in Computer and Information Security (currently enrolled)

Marin Transportation Authority

October 2, 2007 – The Marin Transportation Authority website was hacked into and redirected users to a pornographic site triggered the federal government to initiate a system-wide shutdown of all government sites with a ***CA.GOV*** domain.

The hacker made an adjustment in the DNS server to reroute traffic.

CA DTS was not notified by GSA of the shutdown.

Yuba County

"Yuba County scrambled to contact 70,000 people whose names and personal information were on a laptop computer stolen from the new Child Support Services office in Linda.

County officials said the stolen laptop contained SSNs, birth dates, driver's license numbers…"

Appeal-Democrat

El Dorado County

June 2007 - “I want you to read this message very carefully, and keep the secret with you till further notice, You have no need of knowing who I am or neither where am from, till I make out a space for us to see, I have being paid $50,000.00 in advance to terminate you with some reasons listed to me by my employers…. “

“please if you have not known God try and go closer to him because one of my boys nearly gunned you down two days ago“

It was determined this email was created and sent from Hong Kong, China

Information Security Strategic Plan (ISSP) 2008/2009

ISSP 2008/2009

- Created March 2008
- Used as a road map for a permanent Security Program
- Outlines major goals that need to be accomplished for the Security Program
- Leverages existing resources within EDC to become more involved and accountable for security within respective organizations

Strategic Goals

Goals are Achieved Through

Following Best Practices, Industry Standards, Regulatory Compliance, etc.

Health Insurance Portability and Accountability Act (HIPAA)

ISO 27002

CA State Administration Manual (SAM)

Privacy Office

CCISDA

CERT

SANS

Etc.

Strategic Goals

1. Develop, Approve, and Promote a Comprehensive Information Security Policy Suite.
1. Ensure All Employees are Aware of their Information Security Responsibilities.
2. Establish Oversight Authority for Information Security for Each Department.
3. Establish a Process for Regular Progress Reporting to Executive Leadership.
4. Implement Controls Enabling Countywide Compliance of Mandated Regulations.
5. Implement and Enhance Business Continuity and Disaster Recovery Programs

Strategic Goals

Develop, Approve, and Promote a Comprehensive Information Security Policy Suite

Enterprise-wide Security Policies

Employee Termination Policy
Information Classification Policy
Server Security Policy
Business Continuity Policy
Incident Response Policy
Risk Assessment Policy

Strategic Goals

Ensure All Employees are Aware of their Information Security Responsibilities

Security Awareness Training

Initial Orientation

Instructor-Led Annual Security Awareness

Newsletters

Web Site

Agency-Wide Email Messages

Computer Based Training

Strategic Goals

Establish Oversight Authority for Information Security for Each Department

Departmental Security Officer

Local Oversight and Governance

Security Services and Local Deployment

Related Planning

Departmental Technical Accountability

Acts as Liaison

Strategic Goals

Establish a Process for
Regular Progress Reporting to Executive Leadership

Primary Departmental Players

Information Technologies
Risk Management
Human Resources (Privacy Office)
County Counsel
Board of Supervisors
Health Depts. (HS, PH, MH)

Strategic Goals

Implement Controls Enabling Countywide Compliance of Mandated Regulations

HIPAA

Federal Rules of Civil Procedure (FRCP)

Email Encryption

Email / Electronic Document Retention

Risk Management

Business Continuity

Disaster Recovery

Strategic Goals

Implement and Enhance

Business Continuity and Disaster Recovery Programs

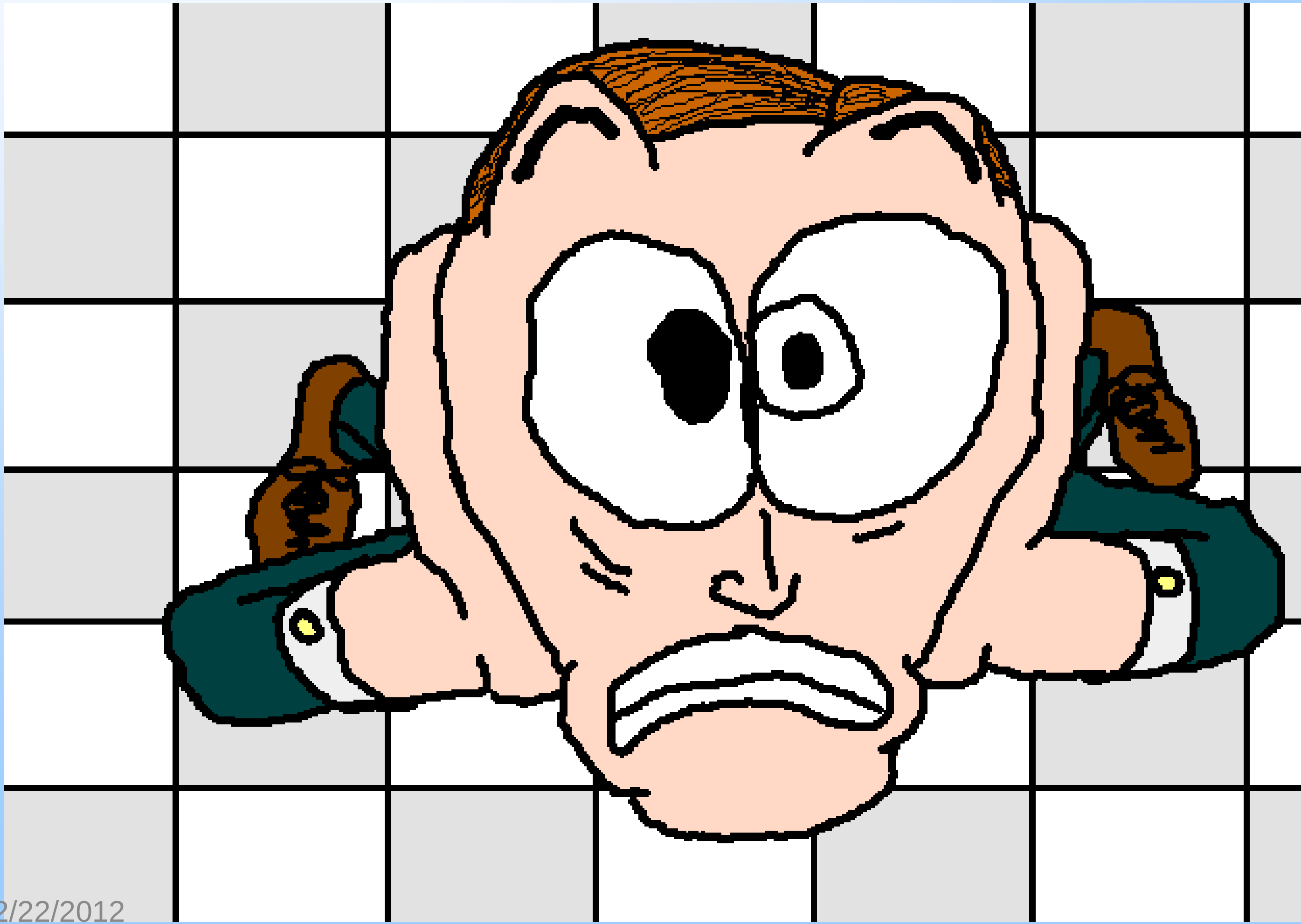
Continuity of Government Operations (COOP)

How To Stay in Business in the Event of a Disaster

Disaster Recovery

Resume Normal Computing Capabilities in as Little Time as Possible Following a Disaster

ISSP Challenges



ISSP Challenges

Significant Resource, Personnel, and Related Budget Issues

Governance Issues

Regulatory Environment

Sheer Volume of Computer Systems

Volume of Data

Ever Changing Vulnerabilities

First 100 days

- **Create the Security Governance Structure**
- **Identify Information Security Officers within each Dept**
- **Develop a Security Awareness and Training Plan**
- **Report Back to Board of Supervisors with Results and Progress**

What Now?

Reviewed by IT Mgmt

Reviewed by Privacy Office

Reviewed by ITSSC

Reviewed by ITSC

Submit to and receive feedback from the Board Of Supervisors to Implement

QUESTIONS?