Security Staffing Discussion Outline

1. Creating a Case for Security Staffing
    a. Summary
        i. System Integrity, Security, and Availability
        ii. Security awareness
        iii. Incident responses
        iv. Compliance
        v. Governance
    b. Existing staff not equipped to develop necessary expertise in the development and implementation of Security matters.
    c. State Agency Comparison
        i. Demonstrate current security FTE from other agencies along with their pending requests for more.
    d. Office of State Auditor
        i. Part of Colorado General Assembly
        ii. Performs IT performance audits of State Agencies, needs to adhere to same standards
    e. Were fortunate to have security conscious advocate on the Joint Budget Committee
2. Key tasks Information Security Analyst has done
        i. Security Awareness Training for all General Assembly Staff
        ii. Information Security Plan
        iii. Get in the way of everyone (e.g. PMs, Sys Ads, Devs, Bas) w/ Forms/Check lists of questions to ask on new projects/tasks
            1. Impact assessment
            2. What type of data (e.g. PII, etc…)
            3. Who needs to access it?
        iv. Assist with incident response
        v. Advocate for cultural change
3. Top 3 things to do if you cannot get a dedicated Information Security Analyst?
    a. Security Awareness Training
        i. Lots of YouTube videos available
            1. May be difficult to track
    b. Antivirus
        i. Minimize the number of solutions in place
        ii. Keep them up to date
    c. Security of Backup Solution
        i. Increased frequency helpful against Ransomware attacks

Document:C.R.S. 24-37.5-404.7

C.R.S. 24-37.5-404.7

Copy Citation

Current through all Laws passed during the 2018 Legislative Session

Colorado Revised Statutes TITLE 24. GOVERNMENT - STATE GOVERNOR'S OFFICE ARTICLE 37.5. OFFICE OF INFORMATION TECHNOLOGY PART 4. INFORMATION SECURITY

24-37.5-404.7. General assembly - information security plans

(1) The general assembly shall develop an information security plan. The information security plan shall provide information security for the communication and information resources that support the operations and assets of the general assembly.

(2) The information security plan shall include:

(a) Periodic assessments of the risk and magnitude of the harm that could result from a security incident;

(b) A process for providing adequate information security for the communication and information resources of the general assembly;

(c) Information security awareness training for regular employees of the general assembly;

(d) Periodic testing and evaluation of the effectiveness of information security for the general assembly, which shall be performed not less than annually;

(e) A process for detecting, reporting, and responding to security incidents consistent with the information security policy of the general assembly. The general assembly and the chief information security officer shall establish the terms and conditions by which the general assembly shall report information security incidents to the chief information security officer.

(f) Plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the general assembly in the event of a security incident.

(3) The legislative service agency directors shall maintain the information security plan pursuant to this section and keep the joint technology committee advised of the plan.

(4) Nothing in this section shall be construed to require the general assembly to adopt policies or standards that conflict with federal law, rules, or regulations or with contractual arrangements governed by federal laws, rules, or regulations.

(5) The general assembly shall provide regularized security awareness training to inform the regular legislative employees, administrators, and users about the information security risks and the responsibility of employees, administrators, and users to comply with the general assembly's information security plan and the policies, standards, and procedures designed to reduce those risks.

History

Source:

L. 2011: Entire section added, (SB 11-062), ch. 128, p. 431, § 9, effective April 22. L. 2013: (3) amended, (HB 13-1079), ch. 246, p. 1193, § 8, effective May 18.

COLORADO REVISED STATUTES

Content Type:

Terms:

Narrow By: -None-

Date and Time: Aug 30, 2018 05:50:55 p.m. EDT

Request for an Information Security FTE

INTRODUCTION

At present, the Colorado General Assembly does not have a dedicated Information Security resource to perform duties critical to maintaining the integrity, security and availability of critical and essential information systems. Additionally, responsibilities related to developing user security awareness, security incidence response processes, compliance and governance would also fall under the purview of this role. This role will also be charged with internal assessments for identifying security weaknesses and vulnerabilities.

STATE AGENCIES COMPARISON

Compared to other state agencies, the legislature is inadequately staffed to support this critical function. This table provides a quick comparative analysis across the state agencies.

Department	Notes
[redacted]	Currently has [redacted] IT security staff with approval to hire [redacted] additional FTEs in FY16-17
[redacted]	Security duties are distributed amongst several people with an estimated [redacted] FTE working specifically on IT security issues
[redacted]	Currently has [redacted] IT security staff with request to hire [redacted] additional FTE in FY17-18
[redacted]	Request for [redacted] additional FTE in FY17-18 for [redacted], their cybersecurity program, bringing their total FTE count to [redacted]
[redacted]	One dedicated Information Security Officer who manages the staff who do network administration and assist with security

REQUEST

Colorado Legislative Council Staff would like to request 1.0 FTE for FY17-18 for an information security analyst.

2018 and 2017 Documented US Ransomware


THE DENVER POST

SamSam virus demands bitcoin from CDOT, state shuts down 2,000 computers

March 2018

- **Atlanta, Georgia** — **SamSam** ransomware disrupted services in the state capital for more than a week, causing disruptions to the court system, online payment systems, and the police department. Atlanta Mayor Keisha Lance Bottoms called the incident "much bigger than a ransomware attack ... This is really an attack on our government, which means it's an attack on all of us." The $51,000 ransom was not paid, and **weeks** after the infection, some government agencies were using paper and pen to get work done.
- **Baltimore, Maryland** — The Computer Aided Dispatch (CAD) systems that power 911 service were locked up by ransomware, forcing 911 operators to relay information **manually for the 17 hours** the system was out of commission. The vulnerability that let the malware in was a recently opened port that was a "result of an internal change to the firewall by a technician who was troubleshooting an unrelated communication issue."

February 2018

- **Denver, Colorado** — Two thousand Colorado Department of Transportation computers were encrypted by the **SamSam** ransomware, locking employees out of their corporate devices. Here's the kicker: As IT pros wiped and reimaged 20 percent of the affected machines, a different strain of ransomware reinfected those devices, resulting in a **multi-week** infestation.

January 2018

- **Washington, D.C.** — More than a 100 police CCTV cameras were taken offline by "two forms of ransomware." The ransom was not paid, and service was restored within **48 hours**.
- **Farmington, New Mexico** — A **SamSam** ransomware infection locked multiple computers; the ransom (about $35,000) was not paid. Nevertheless, the city was able to recover the encrypted information.
- **Cockrell Hill, Texas** — After refusing to pay the ransom, the police department wiped the infected machines to prevent further damage, resulting in the **loss of seven years of data, including video evidence dating back to 2009**.

December 2017

- **Mecklenburg County, North Carolina (includes Charlotte)** — Multiple computers got hit with **LockCrypt** ransomware, which affected "municipal financial reporting, child support enforcement, transactions processing, and a few more online services." The $23,000 ransom was not paid.

November 2017

- **Spring Hill, Tennessee** — The trouble began when an employee **clicked on a "bad link,"** resulting in a **weeks-long** infection that affected email, accounting, police, emergency dispatch, and online bill payment systems. The $250,000 ransom was not paid, and emergency dispatchers were forced to do their work using dry-erase boards for more than 10 days.

October 2017

- **Issaquah, Washington** — The small city was hit by **CryptoLocker**, which took city services offline for **four days**. The city, which only employed two IT pros at the time, suffered from a "decade of underinvestment of IT," which resulted in the infection. Luckily, they did manage to spend some money on a backup solution (a Unitrends appliance), and they were able to get back up and running, but it required "hundreds of man-hours to recover."
- **Englewood, Colorado** — All internal city systems were shut down because of ransomware, affecting online payment systems and various public facilities. IT pros from the nearby city of Denver pitched in to get them back up and running within **several days**.


Ransomware attack hits city of Englewood

September 2017

- **Montgomery County, Alabama** — Services relating to vehicle registration and the issuance of business and marriage licenses were affected. The county's revenue and district attorney offices were also locked up in the attack.
- **Butler County, Kansas** — Due to an unspecified ransomware infection, 911, law enforcement, and county attorney systems went down. One interesting tidbit from this story: Butler County's insurance provider had allegedly previously "dealt with 100 cases of (ransomware infections) in local government."
- **San Ysidro, California (part of San Diego)** — Hackers demanded $19,000 in Bitcoin to unlock email servers, but the ransom was not paid. Despite disruptions in service, the district was eventually able to restore all files.

August – January 2017

- **Washington, Missouri** — City; **Lawton, Oklahoma** — City; **Murfreesboro, Tennessee** — police and fire departments **Calallen, Texas** — A school district **Memphis, Tennessee** — FedEx **(NotPetya)**; **Cook County, Illinois (Chicago)** — (**WannaCry)**; **Brewer, Maine** — Brewer School Department; **Newark, New Jersey** —city hall; **Atlanta, Georgia** — Atlanta has allegedly been hit by ransomware twice in less than a year. Root cause: SMB bug.; **Buffalo, New York** — Erie County Medical Center; **Mountain Home, Arkansas** —city's water utility service; **Pennsylvania Senate** — The computer network of the Democratic Caucus office; **Licking County, Ohio** — County Courts/police EMS; **Bingham County, Idaho** — County; **Saint Louis, Missouri** — The public library system; **Bigfork, Montana** —public school system.