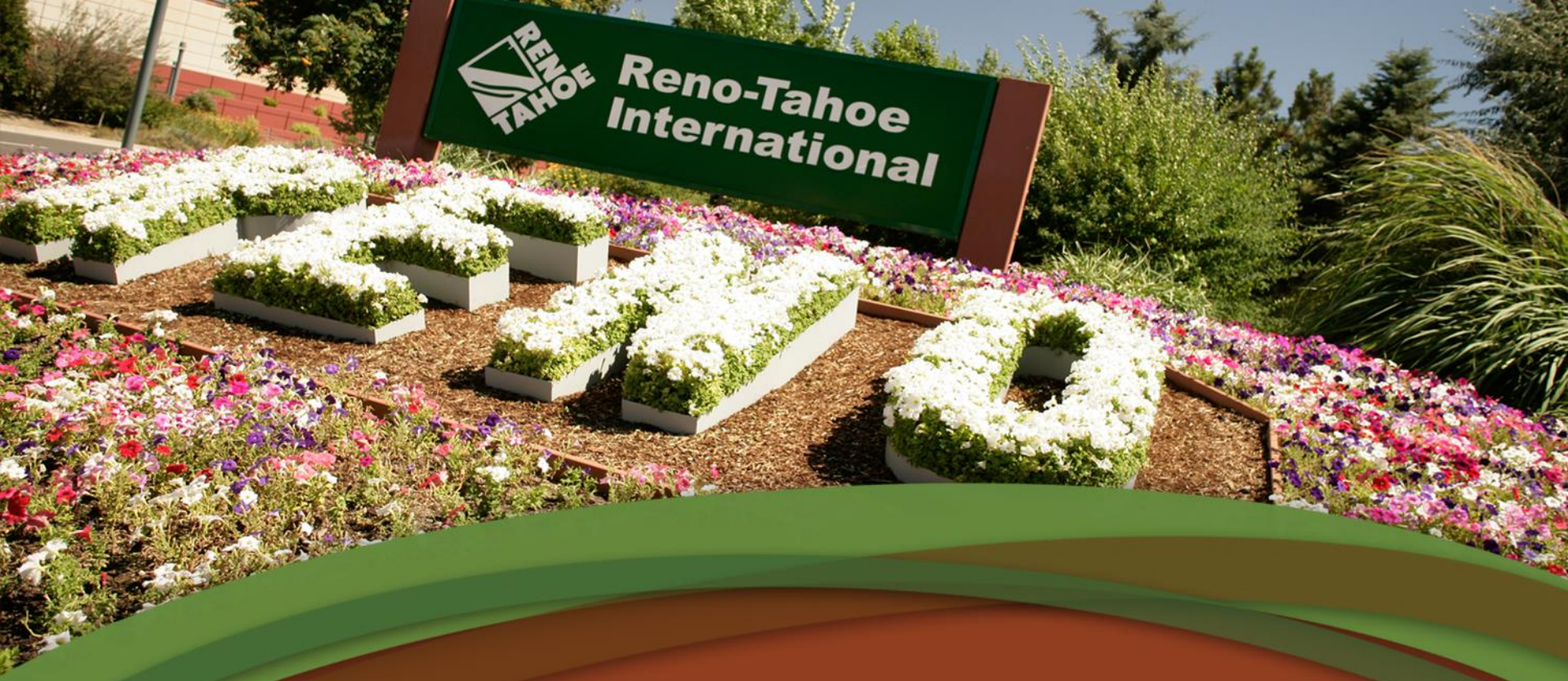


Cyber Security

Martin L. Mueller, CIO

May 4, 2018

Reno-Tahoe Airport Authority

Topics

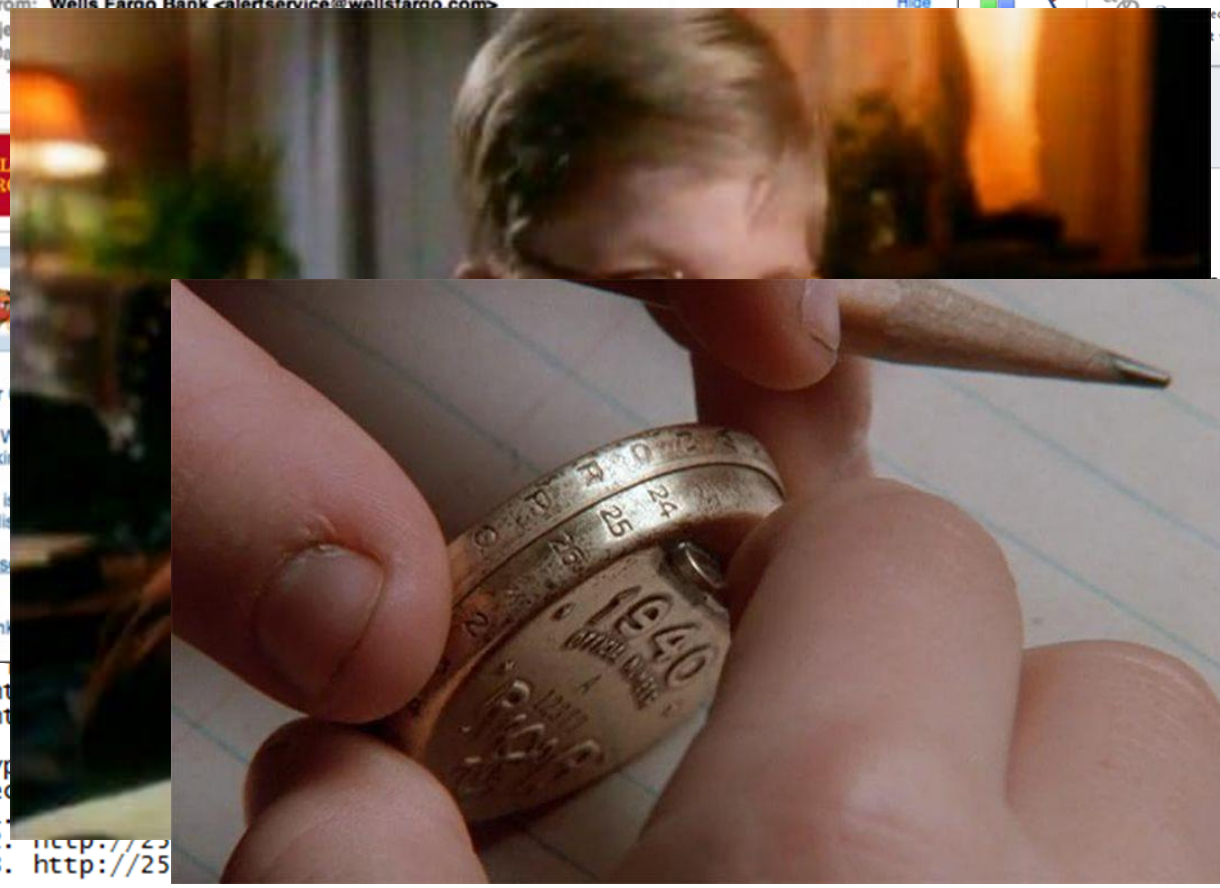
- Ransomware
- Blockchain
- Crypto Currencies
- SSI

Cyber Crime

- "Stranger than Fiction"
  - Eternal Blue, Spectre, Meltdown, Drupal-geddon
  - Experian
  - Facebook
  - State-sponsored cyber warfare/terrorism
- $400B to $1.2T Industry
- Cyber Criminals "Follow the Money"
  - ID Theft >> Sextortion >> RansomWare >> MalMining
  - Phishing >> Spear Phishing >> Whaling

Ransomware

- Break in >> Files Locked >> Extortion
- Results in Days or Weeks of Partial/Full Disruption, Possible Permanent Data Loss
- High Profile Examples
  - Hospitals
  - Police Departments
  - Governments
  - Utilities
  - Airports



Wells Fargo Notification – Message ID:7930826 — Inbox

From: Wells Fargo Bank <alertservice@wellsfargo.com>

Hide

(HTML)

Find

Zoom

Zoom

Sent: Tue 3/29/2016 5:18 PM

our working
ect it from a suspected
e able to put the
les, but we cannot do

ich is on our secret server.

```
    3. http://25

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: 25z5g623wpqpdwis.onion/0E5E84EC58F2D25E
    4. Follow the instructions on the site.

!!! Your personal identification ID: 0E5E84EC58F2D25E !!!
=$_-|*__$~**__==_|
=$*_|_*=|
```

Connect to social networks to show profile photos and activity updates of your colleagues in Outlook. Click here to add networks.

How to Prevent a Ransomware Attack

THE LOCKHEED MARTIN CYBER KILL CHAIN®

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

Stopping adversaries at any stage breaks the chain of attack! Adversaries must completely progress through all phases for success; this puts the odds in our favor as we only need to block them at any given one for success. Every intrusion is a chance to understand more about our adversaries and use their persistence to our advantage.

The kill chain model is designed in seven steps:

- Defender's goal: understand the aggressor's actions
- Understanding is Intelligence
- Intruder succeeds if, and only if, they can proceed through steps 1-6 and reach the final stage of the Cyber Kill Chain®.

A New Approach

Break as Many Links as You Can

- System is compromised
  - Vulnerabilities **Timely Patching**
  - Drive-by Attacks **Education**
- Files are accessed and "encrypted" **Limit Access by Role**
- Service is affected **Business Continuity Planning**
- Extortion attempt **Law Enforcement Relationships**
- Data is restored, or **Verified 3-2-1 Backups**
- Payment is made **Hoard BitCoin?**

What is Blockchain Technology?

- Secure Network Technology
- Peer-to-Peer Database (ledger)
  - Secure
  - Private
  - Verifiable
  - Powerful
  - Supra-National

Blockchain Applications

- Payment Systems: parking, public transit, filing fees, taxes
- Consolidate Medical Record (including insurance and Health and Human Services)
- Licensing and Applications
- Identification and DMV
- Law Enforcement, Justice, and Legal
- Grants and Titles
- Public Records
- Welfare and Social Services
- Asset Management
- E-Commerce
- Finance and Investments
- Crowd Sourcing/Funding
- Digital Copyrights

Blockchain Constraints

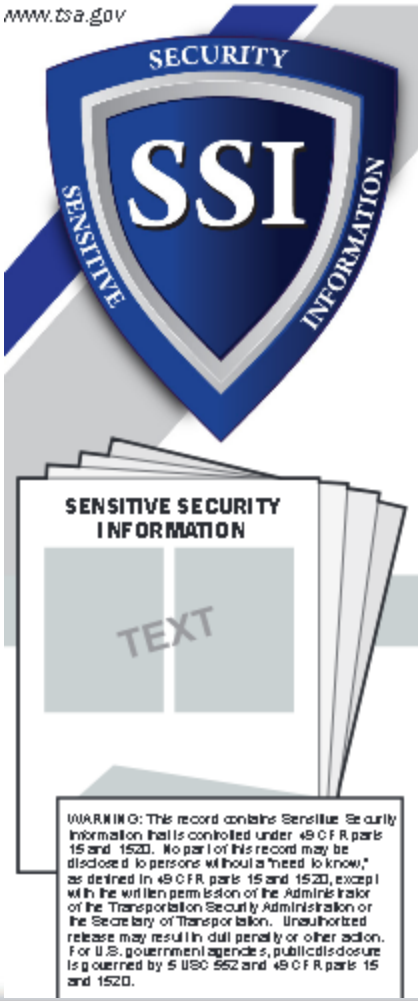
- Security (Estonia)
- Trust (BitCoin, MtGOX, Coincheck)
- Privacy
- Startup Investment
- Resource Constraints
- Political Resistance
- Requires Partnering
- Labor Disruption
- Energy Consumption & Waste
- Governance and Law Enforcement
- Lack of Standardization

What are Cryptocurrencies?

- Currencies based on Blockchain technology
  - Unregulated (peer-to-peer)
  - Trust based (not "backed" or insured)
  - Private and untraceable
    - Legitimate Business Transactions
    - Circumvent Censorship/Oppression
    - Commit Crime
      - Child abuse
      - Human trafficking
      - Drug trafficking
      - Violent crime
    - Support Terrorism

Security Sensitive Information (SSI)

www.tsa.gov



Sensitive Security Information

Best Practices Guide for Non-DHS Employees and Contractors

The purpose of this hand-out is to provide *transportation security stakeholders and non-DHS government employees and contractors* with best practices for handling SSI. Best practices are not to be construed as legally binding requirements of, or official implementing guidance for, the SSI regulation.

What is SSI?

Sensitive Security Information (SSI) is information that, if publicly released, would be *detrimental to transportation security*, as defined by Federal regulation 49 C.F.R. part 1520.

Although SSI is not classified information, there are specific procedures for recognizing, marking, protecting, safely sharing, and destroying SSI. As persons receiving SSI in order to carry out responsibilities related to transportation security, you are considered "covered persons" under the SSI regulation and have special obligations to protect this information from unauthorized disclosure.

SSI Requirements

The SSI regulation mandates specific and general requirements for handling and protecting SSI.

You Must – Lock Up All SSI: Store SSI in a secure container such as a locked file cabinet or drawer (as defined by Federal regulation 49 C.F.R. part 1520.9 (a)(1)).

You Must – When No Longer Needed, Destroy SSI: Destruction of SSI must be complete to preclude recognition or reconstruction of the information (as defined by Federal regulation 49 C.F.R. part 1520.19).

You Must – Mark SSI: The regulation requires that even when only a small portion of a paper document contains SSI, every page of the document must be marked with the SSI header and footer shown at left (as defined by Federal regulation 49 C.F.R. part 1520.13). Alteration of the footer is not authorized.

SSI (continued)

Best Practices Guide

Reasonable steps must be taken to safeguard SSI. While the regulation does not define reasonable steps, the TSA SSI Branch offers these best practices as examples of reasonable steps:

- Use an SSI cover sheet on all SSI materials.
- Electronic presentations (e.g., PowerPoint) should be marked with the SSI header on all pages and the SSI footer on the first and last pages of the presentation.
- Spreadsheets should be marked with the SSI header on every page and the SSI footer on every page or at the end of the document.
- Video and audio should be marked with the SSI header and footer on the protective cover when able and the header and footer should be shown and/or read at the beginning and end of the program.
- CDs/DVDs should be encrypted or password-protected and the header and footer should be affixed to the CD/DVD.
- Portable drives including "flash" or "thumb" drives should not themselves be marked, but the drive itself should be encrypted or all SSI documents stored on it should be password protected.
- When leaving your computer or desk you must lock up all SSI and you should lock or turn off your computer.
- Taking SSI home is not recommended. If necessary, get permission from a supervisor and lock up all SSI at home.
- Don't handle SSI on computers that have peer-to-peer software installed on them or on your home computer.
- Transmit SSI via email only in a password protected attachment, not in the body of the email. Send the password without identifying information in a separate email or by phone.
- Passwords for SSI documents should contain at least eight characters, have at least one uppercase and one lowercase letter, contain at least one number, one special character and not be a word in the dictionary.
- Faxing of SSI should be done by first verifying the fax number and that the intended recipient will be available promptly to retrieve the SSI.
- SSI should be mailed by U.S. First Class mail or other traceable delivery service using an opaque envelope or wrapping. The outside wrapping (i.e. box or envelope) should not be marked as SSI.
- Interoffice mail should be sent using an unmarked, opaque, sealed envelope so that the SSI cannot be read through the envelope.
- SSI stored in network folders should either require a password to open or the network should limit access to the folder to only those with a need to know.
- Properly destroy SSI using a cross-cut shredder or by cutting manually into less than ½ inch squares.
- Properly destroy electronic records using any method that will preclude recognition or reconstruction.

Transportation Security Administration

Phone: (571) 227-3513 ▪ Fax (571) 227-2945

Safely Sharing Information

SSI@dhs.gov

Resources

- Eternal Blue
  - https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/
- Cost of cyber crime
  - https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
- Cryptography
  - Singh, Simon (2016), The Code Book, ISBN *9780385730624*
- Killchain analysis
  - https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- Blockchain and Cryptocurrency
  - https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world
  - https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector
  - https://blockgeeks.com/guides/what-is-cryptocurrency/
- Excellent Cyber Resources
  - https://www.nist.gov/topics/cybersecurity
  - https://www.us-cert.gov/ncas/tips
  - http://www.dhs.gov/cybersecurity-tips
- Security Sensitive Information
  - https://www.gpo.gov/fdsys/pkg/CFR-2011-title49-vol9/pdf/CFR-2011-title49-vol9-part1520.pdf
  - https://www.tsa.gov/for-industry/sensitive-security-information

Questions?

Reno-Tahoe Airport Authority