Why You Should Be Losing Sleep Over Cybersecurity
League of California Cities City Managers Department Meeting

Moderated by Lea Deesing, Chief Innovation Officer for the City of Riverside

George Khalil,
Chief Information Security Officer,
City of Riverside

Mitch Cochran,
IT Director,
City of San Bernardino

GEORGE KHALIL

• 20 years in IT
• Has public service and fortune 500 experience
• His efforts led to Riverside winning ICMA Excellence Award in 2017
• He is a certified intrusion analyst, incident handler, network, and systems auditor, Forensic Analyst, Penetration Tester, Project Manager, and Certified Security Expert
• Received national recognition for his 2017 Western Cities article on Cybersecurity
• Is a nationally-recognized speaker on cybersecurity
• Serves on several advisory boards and committees
MITH COCHRAN

- City of San Bernardino Director of Technology
  - 21 Years of Municipal IT Management, both large and small
  - Orange County Courts
  - IBM Systems Engineer
- CISM, CGCIO
- Masters in Administration, Masters in Homeland Security
- University Lecturer / Author
- Officer in the California State Military Reserve

GEORGE KHALIL
Chief Information Security Officer
City of Riverside
• How many of you have a full time employee dedicated to cybersecurity?
• How many don’t know whether they have a full time employee dedicated to cybersecurity?
• Today I’ll be highlighting some of the reasons why you need one.

CIS 20 Critical Controls

CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organization’s vulnerabilities

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges
Pervasive Threats?

CIS Control 13
Data Protection

• Key Principle:
• The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
**Pervasive Threats?**

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, **the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error.** Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

---

**BOEING EMPLOYEE EMAILS**

36,000 COWORKERS’ PERSONAL INFO TO SPOUSE

ACCIDENTALLY LEAKED CREDENTIALS; MISPLACED DATA

Boeing has started notifying the 36,000 employees whose personal information was mistakenly leaked via email, according to Threatpost.

A Boeing employee had a problem formatting a spreadsheet and emailed it to his spouse for help, wrote Boeing Deputy Chief Privacy Officer Marie Olson in a letter to the Washington State attorney general notifying the state of the data breach.

The spreadsheet contained names, birthdates, Social Security numbers, and other accounting code and employee identification information—but tucked away in “hidden” columns. The employee sent the email Nov. 21, though it wasn’t discovered until January.

Boeing is offering employees two years of identity protection services.
Pervasive Threats?

Personal information of almost 200 million registered U.S. voters was accidentally exposed online due to an improperly configured security setting, security firm UpGuard revealed on Monday.

The leaked information, compiled by Republican data firm Deep Root Analytics and two other Republican contractors, included names, birth dates, addresses, voter registration details and social media posts.

UpGuard cyber risk analyst Chris Vickery discovered the open database of 198 million voters on June 12, and it was secured on June 14. Putting that number into context, Politico reported last October that the United States had a little more than 200 million voters.

About 1.1 terabytes of data was available to download and not password protected.

Security

Yet another AWS config fumble: Time Warner Cable exposes 4 million subscriber records

US cable giant the latest victim of S3 cloud security brain-fart
Pervasive Threats?

Healthcare IT News

Privacy & Security

Accenture latest to breach client data due to misconfigured AWS server

Hundreds of gigabytes of sensitive client and company data were exposed when the tech and cloud giant accidentally left four of its AWS S3 buckets open to the public.

---

63% of Data Breaches Result From Weak or Stolen Passwords

In its recent 2016 Data Breach Investigations Report, Verizon Enterprise confirmed many industry trends that we see at ID Agent every day. The most glaring blind spot for organizations is how stolen credentials are the primary means by which hackers exploit their vital systems.

Credentials are the holy grail for hackers. In a study of 905 phishing attacks, the vast majority—91 percent—were after user credentials.
L.A. County targeted in phishing cyberattack; private information of 750,000 people compromised

The San Francisco Rail Ransomware Rogue Has Been Hacked... Twice

Thomas Fox-Brewster, FORBES STAFF
“Muni would lose an estimated $559,000 for every day that it was unable to collect fares, according to its operating budget (see Ransomware Extortion: A Question of Time).”
Cyberattack Targets San Jose Police Department, City Websites

By Jennifer Wadsworth @jennwadsworth / November 9, 2015

A map of DDoS cyberattacks from around the world. (Screen capture via Digital Attack Map)

---

TECHNOLOGY NEWS | Thu Feb 25, 2016 | 6:52pm EST

U.S. government concludes cyber attack caused Ukraine power outage

By Dustin Volz | WASHINGTON

A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognized the blackout as caused by a malicious hack.
By HOLLY WILLIAMS / CBS NEWS / December 21, 2016, 7:27 PM

Russian hacks into Ukraine power grids a sign of things to come for U.S.?

City, streetcar project scammed for $3.2 million

Elida S. Perez, El Paso Times   Published 1:07 p.m. MT Nov. 2, 2016 | Updated 6:40 p.m. MT Nov. 2, 2016

Crews work on the Downtown El Paso trolley project along Kansas Street and Mills Avenue. Ruben R. Ramirez/El Paso Times
WHO HAS ACCESS TO YOUR DATA?

IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
What constitutes protected data?

- PII (SSN, DL, Medical, Username and password, Credit card)
- CIVIL CODE - CIV
- DIVISION 3. OBLIGATIONS [1427 - 3272.9]
  - ( Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14. )
- PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273]
  - ( Part 4 enacted 1872. )
- TITLE 1.8. PERSONAL DATA [1798 - 1798.78]
  - ( Title 1.8 added by Stats. 1977, Ch. 709. )
- CHAPTER 1. Information Practices Act of 1977 [1798 - 1798.78]
  - ( Chapter 1 added by Stats. 1977, Ch. 709. )
- ARTICLE 7. Accounting of Disclosures [1798.25 - 1798.29]
  - ( Article 7 added by Stats. 1977, Ch. 709. )
  - 1798.29.

- Other protected Data (HIPPA, PCI, CJIS, CELTS, GDPR, PHI, NERC, Gramm-Leach-Bailey Act, FERPA and others)
- Business sensitive information that can cause harm if exposed
- National Security or classified material
- Intellectual property
- CAD, Diagrams or design documents
What are employees doing with your data?

HUFFPOST

POLITICS

Adelaide Security Breach Sees Secrets Stolen From International, $1.1 Trillion Joint Strike Fighter Project

Using "admin-admin" as your login-password is ridiculous.
① 12/10/2017 8:46 AM AEDT | Updated 12/10/2017 9:59 AM AEDT

What are employees doing with your data?

COMPUTERWORLD

EVEN ONE UNSECURED PRINTER CAN PUT YOUR COMPANY AT RISK. Assess the risks to your network.

Home > Security

NEWS

Classified U.S. military info, corporate data available over P2P

Inadvertent data leakage worse than thought, experts tell Congress
What are employees doing with your data?

Russian spies used Kaspersky AV to hack NSA staffer, swipe exploit code – new claim

"What are the hell are these people thinking?” asks Aitel. "Leaving the NSA with top-secret documents and putting them on your home machine is the very first thing they tell you not to do. Why it keeps happening is a mystery to me, and probably to the management at NSA.”

ANDY GREENBERG, WIRED.COM 10.05.17
What are employees doing with your data?

Laptop Theft May Have Exposed PHI of 400,000 Current or Former California Inmates

June 7, 2016 by Heather Landi

The theft of a non-encrypted laptop belonging to a staff member of California Correctional Health Care Services may have exposed the protected health information (PHI) of up to 400,000 patients who served time in California prisons during an 18-year period.

3rd Party risk?

OPINION

Hackers are aggressively targeting law firms' data

If you thought hackers were afraid of the guys who can prosecute them, think again!
Cyberattacks once again roil Hollywood, but can anything be done about it?

By David Ng, Ryan Faughnder and Parekh Dave - Contact Reporters

Like most large corporations, major Hollywood studios are fond of outsourcing. From coming attraction trailers that are designed to draw audiences into cinemas to eye-popping 3-D visual effects that burst off the screen, studios routinely farm out large chunks of work to vendors around the globe who compete to provide lowest-cost solutions.

And therein lies a big cybersecurity problem, according to experts. Hackers increasingly are targeting these vendors to piller movies and TV series prior to their releases. The cyberthieves are betting — correctly in some cases — that lax network security at these vendors will allow easy access to content that they can hold hostage for a ransom.

6.7 Million Voter records

Researcher discovers Georgia voter database exposed online

By Associated Press  June 15, 2017 | 2:41am
Do we even know where our data lives?

<table>
<thead>
<tr>
<th>Category</th>
<th>Bank/Credit/Financial</th>
<th>State</th>
<th>Breach Category</th>
<th>Records Exposed?</th>
<th>Exposed # of Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>UT</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>MI</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>MN</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>WA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>PA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>TX</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>MA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>WA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>TX</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>CA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>FL</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>CA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>CO</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>DE</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>TX</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>CA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>CA</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
<tr>
<td>NY</td>
<td>Bank/Credit/Financial</td>
<td>Yes</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

How is this report produced? What are the tables? See last page of report for details.

Report Date: 10/15/2017
Do we even know where our data lives?

<table>
<thead>
<tr>
<th>Reference</th>
<th>Business</th>
<th>Data Disclosure</th>
<th>State</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR2017BS4</td>
<td>Yes</td>
<td>Yes</td>
<td>NY</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS43</td>
<td>Yes</td>
<td>Yes</td>
<td>FL</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS44</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS45</td>
<td>Yes</td>
<td>Yes</td>
<td>MA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS46</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS47</td>
<td>Yes</td>
<td>Yes</td>
<td>TN</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS48</td>
<td>Yes</td>
<td>Yes</td>
<td>ID</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS49</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS50</td>
<td>Yes</td>
<td>Yes</td>
<td>NY</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS51</td>
<td>Yes</td>
<td>Yes</td>
<td>IN</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS52</td>
<td>Yes</td>
<td>Yes</td>
<td>IA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS53</td>
<td>Yes</td>
<td>Yes</td>
<td>NY</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS54</td>
<td>Yes</td>
<td>Yes</td>
<td>FL</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS55</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS56</td>
<td>Yes</td>
<td>Yes</td>
<td>KY</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS57</td>
<td>Yes</td>
<td>Yes</td>
<td>IL</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS58</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS59</td>
<td>Yes</td>
<td>Yes</td>
<td>NY</td>
<td>Business</td>
</tr>
<tr>
<td>FR2017BS60</td>
<td>Yes</td>
<td>Yes</td>
<td>CA</td>
<td>Business</td>
</tr>
</tbody>
</table>

Report Date: 10/15/2017

Unknown
What do they have in common?

• They all have:
  – Firewalls
  – Antivirus
  – They Patch (at least some systems)
  – They train their employees
  – They don’t know where their data lives
  – They lack the capability to determine what data was lost

What do they have in common?

Did they lose sight of what they are supposed to protect?
Don’t get stuck in the how and forget why

Can anyone protect this?
George’s 21st Critical Control

“Know thyself.”
- Socrates
- George

Enterprise Data Security Challenges

• We all know where data should be stored
• But most of us don’t know where data is stored
• Security operates in a continuous incident response loop
• The business does not understand the impact of a data breach
• Cleanup is a massive undertaking
Data Protection

• Establish Sensitive data handling policy
  – Establish sensitivity classification
  – Create document templates
  – Create watermarks, labels and meta data standards
  – Identify employee roles and restrict access
  – Update and enforce your data retention policies
    • You can’t lose what you don’t save

Data Protection

• Review legacy data
  – Automatic discovery and classification of stored data
    • Include network shares and email
    • Desktops
    • Laptops
    • Mobile devices
    • Servers
    • Enterprise applications
    • Don’t forget the Cloud
Data Protection

- Engage your business
  - IT and Security are not the data custodians
  - Each business unit that generates data needs a Data Champion
  - Review how each business unit generates sensitive data
    - Most data is redundant and not needed
    - You often encounter duplicate records, reports, and orphan files
    - Change risky business processes
    - Enforce your record retention policies

Data Protection

- You can’t lose what you don’t have

Remember:

Everything you save can and will be used against you in the event of a breach.
MITCH COCHRAN
Director for Information Technology
City of San Bernardino

Topics

• CISO – Chief Information Security Officer
• Budget Issues
• The Value is in the Network
• Internet of Things
• Evaluating Security
• What is in the Future - Disinformation
A chief information security officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

Most organizations don’t have enough resources. Should we dedicate a person to be a CISO?

– It is a very similar issue to website and communications issues. Do you have webmaster?

– Security is only going to get more complex
  • More regulations
  • More technicalities to understand in the technology
  • More connections
  • Are new systems being implemented with security in mind?

– How can these responsibilities be covered
Budget

• IT has as much or more deferred maintenance than any other department.
  – We can wait on replacing those PCs.
    • PC’s should be replaced about every 4-5 years, many are 8 years old.
    • Servers should be replaced about every 6 years, some are 10 years or more old.

• It is similar to street maintenance, the longer you put it off, the more it will cost.

Budget

• The biggest issue is all of the hardware and software is interdependent
  – If upgrades are delayed, then other upgrades may be prevented.
  – Vendors require specific versions
    • Sometimes old ones which limit us
    • Sometimes new ones which force us into upgrades

• Windows XP – unsupported as of April 2014
• Windows 7 – unsupported as of Jan 2020
  – So all workstations need to go to Windows 10
Budget

• Departments as a cost center
  • Each department chooses to defer so they can put money other places
• Better to fund it as a corporate asset
  • Easier to manage across departments, ensure that workstations and software are kept up to date
• CapEx vs OpEx - What makes sense for your organization?
  • Are hosted solutions better with a predictable annual cost?
  • Are one-time costs better since they will be less expensive over time
  • Leasing workstations costs more but it forces you to replace them on the schedule.
  • Hosted software – lower initial cost, but it be required every year
    – Hosted programs may have different levels of functionality than desktops

The Value is in the Network

• Numerous applications are about gathering information from numerous sources.
• From the security perspective
  – My network is susceptible to any vulnerabilities that my partners have
  – The Target Store hack started with the HVAC subcontractor
IOT - Internet of Things

• Everything can be connected to the Internet
• We can envision incredible opportunities
  – But we have to protect everything
    • We have to be right 100%, the bad guy one time
  – If you can see the doorbell from your phone, so can a hacker
    • There will be security holes
  – Security is sometimes forced to the lowest common denominator - which may be no security
    • The business need trumps the security implementation

The Network is New and Old at the Same Time

• We will be connecting technology that is old
  – Industrial equipment has long life spans
  – HVAC, traffic signal controllers, radios
• It was not designed with security in mind
• There are few updates
• Even new cars are not designed with security in mind
  – It is getting better but there is a long way to go
Evaluating Security

- In our litigious society
  - Deep pockets will be sued, someone is at fault
  - Lawsuits have the luxury of being a Monday morning quarterback
    - You should have known, you are an expert
    - You should have foreseen it coming
    - If you followed every regulation or suggested best practice, it would not have happened
- We need to be proactive with demonstrated actions
- MISAC Excellence in IT Practices program
  - A free audit

The Feds - 171 - A new Standard?

- A federal security directive will require businesses working with the federal government to protect their cyber data, or have a detailed plan for doing so, by Dec. 31, 2017.
- The directive is called “NIST 800-171 Rev.1” or just rule 171.
- It will control whether companies from defense engineering firms to janitorial outfits can do business with the federal government.
What’s Next - Disinformation

• The expectation is that cyber warfare is evolving to disinformation
• Previous cyber-incidents focused on information acquisition, network infiltration or precision strikes to sabotage the opposition.
• What we are seeing now are disruptive cyber-actions with the goals of disrupting normal systems and demonstrating the instability of Western democratic models

Victory in information warfare “can be much more important than victory in a classical military conflict, because it is bloodless, yet the impact is overwhelming and can paralyze all of the enemy state’s power structures”
• Defense Minister Sergi Shoigu said that Russian “Information Troops” were involved in “intelligent, effective propaganda”
Cyber Strategies

• Cyber-strategies have now become indirect forms of coercion designed to weaken adversary resolve and create uncertainty, as well as undermine alliances or create political wedges.

When is an Attack an Act of War?

• Interference with an election is not an act of war.
• The Russians purchased 3000 ads.
  – Then used normal Facebook tools to maximize the impact
  – They were friending the information among their accounts
  – The ad looked real and is hard to distinguish from a normal post.
Speed of Information

- Think of how much information gets posted.
- Think of how fast information gets posted
  - And re-posted
  - Who is that source?

CITY MANAGER ACTION ITEMS

- Embrace change, support a risk-aware culture
- Support a cyber security awareness training and testing program
- Hire a CISO, if you can
- Vet cloud software by requiring departments to use a “Software as a Service Checklist”
- Vet vendors thoroughly
- Require cyber liability insurance
- Implement a data loss prevention program
CITY MANAGER ACTION ITEMS

- Support technology lifecycle/replacement programs
- Receive free yearly audits through the MISAC Excellence in IT Practices Award application
- Ensure your staff are following best practices
- When notified of cybersecurity weaknesses take immediate action
- Understand the laws surrounding transparency and document retention requirements

CONTACT INFO & QUESTIONS

George Khalil:  gkhalil@riversideca.gov
Mitch Cochran:  Cochran_Mi@sbcity.org
Lea Deesing:  ldeesing@riversideca.gov