Lessons in Cybersecurity from the Hacker's Playbook

CSMFO

SPEAKER PRESENTATION

YESTERDAY, TOMORROW AND FINANCE
2020 CSMFO ANNUAL CONFERENCE
JANUARY 28-31, 2020
DISNEYLAND CA

Lessons in Cybersecurity from the Hacker's Playbook

Kerry Benson, PFM
Managing Director & Chief Information Officer

Carl Sandstrom, California Joint Powers Insurance Authority
Business Projects Manager

An Impressive Business Profile

+11%
increase in the last year

145
average number of security breaches in 2018

130
average number of security breaches in 2017

=67%
Increase in the last 5 years

$13.0m
average cost of cybercrime in 2018

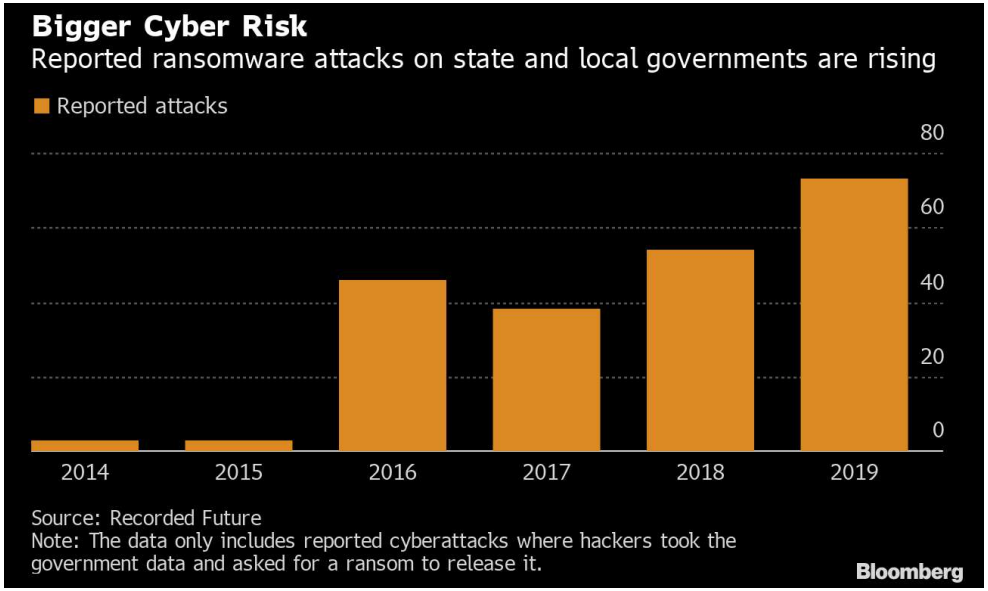
=72%
Increase in the last 5 years

Hacking is a business
ENTERPRISE.

Source: Accenture Security Ninth Annual Cost of Cybercrime study.

Government Attacks on the Rise

"Ransomware incidents increased sharply in 2019 **due to organizations' existing security weaknesses** and the development of increasingly sophisticated attack mechanisms specifically designed to exploit those weaknesses. Combined, these factors created a **near-perfect storm**."



Source: Emisoft, 2019.

Public Sector at High Risks

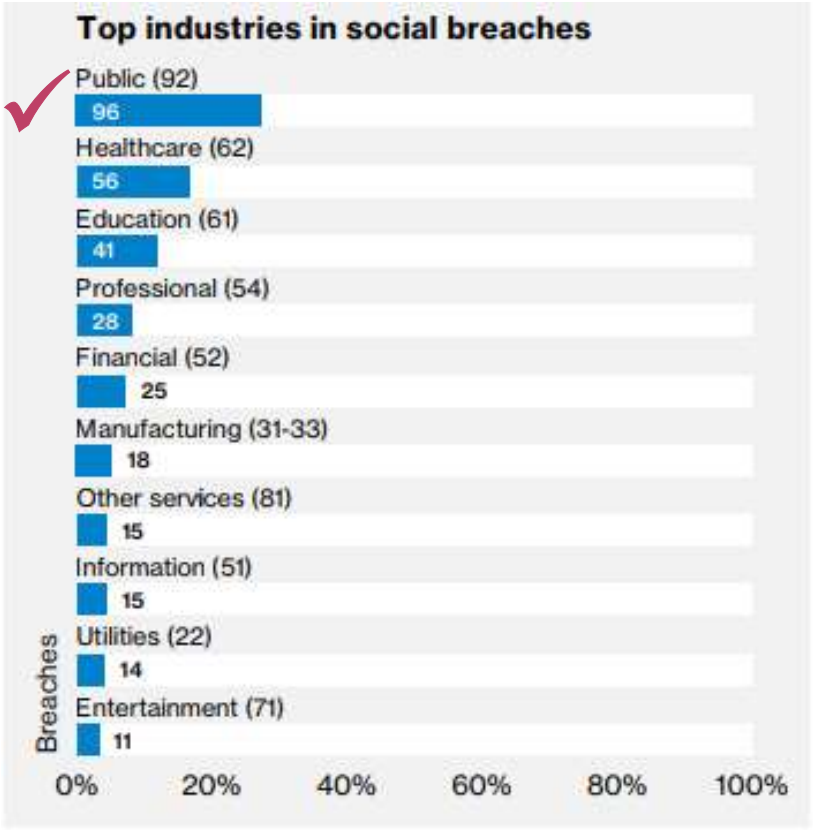


Figure 11. Top industries within Social breaches (n=351)

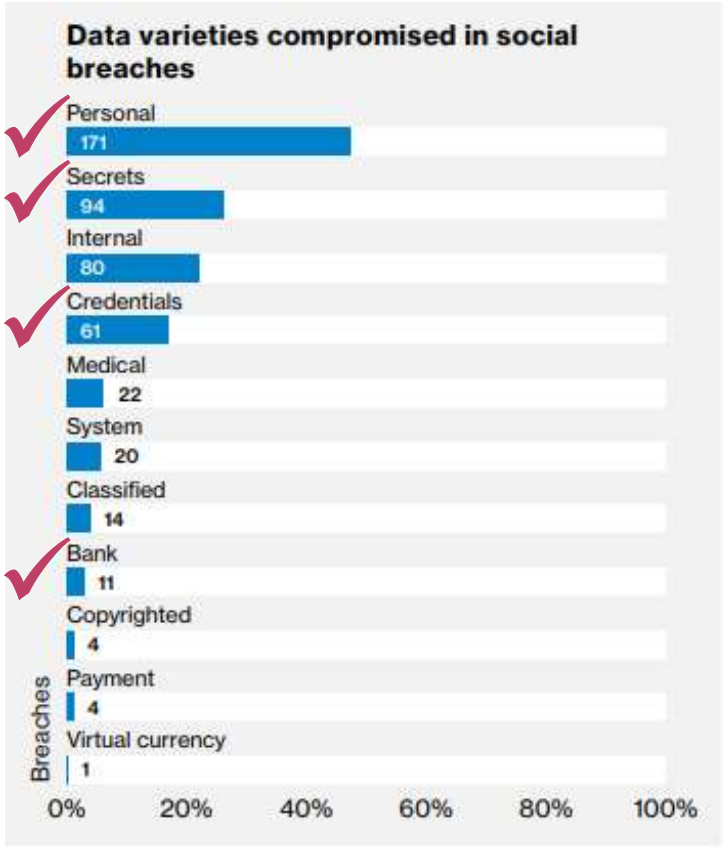


Figure 12. Data varieties compromised in Social breaches (n=362)

Source: 2018 Data Breach Investigations Report 11th edition.

Why are Cities More Vulnerable?

- ✓ Less security
- ✓ More attack vectors
- ✓ Higher value data
- ✓ Larger volume of data
- ✓ Critical public services at risk

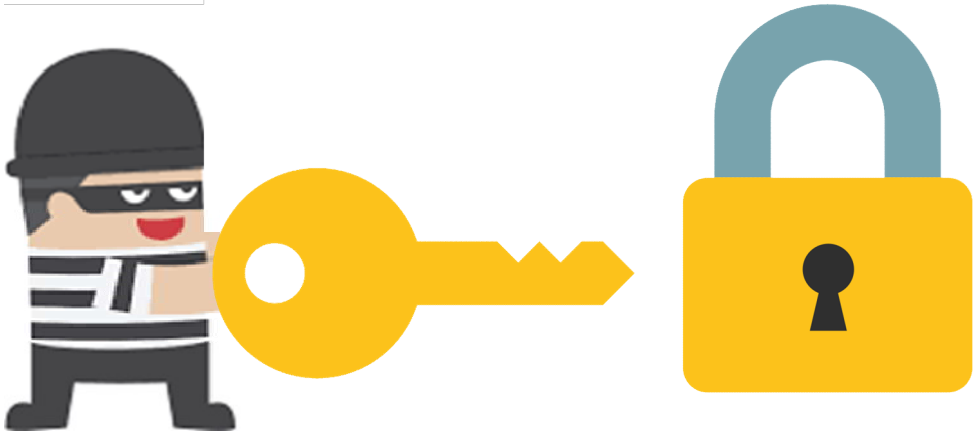
*"Local and federal government entities have suffered **443** data breaches since 2014, with last year being the worst year on record."*

California is the top state for data breaches, likely due to being the home to more tech and internet companies than others

Source: Comparitech, 2019.

The Anatomy of an Attack

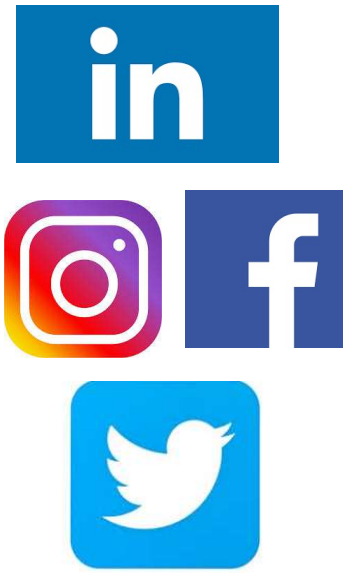
1. Online Reconnaissance
2. Probe for Points of Access
3. Exploit Vulnerabilities
4. Infiltrate the Network
5. Spread on the Network
6. Hide all Evidence



Entity Research

- What does the organization do?
- Who are the key executives and employees?
- Who are key customers, vendors and affiliates?
- How do critical processes work?
- What are the critical systems?
- What financial resources do they have or control?
- What sensitive information exists?
- How sophisticated is the entity?
- Where are they located?
- Is there information on the dark web about the entity?

Executive and Employee Research



- Professional:
  - Where do they sit in the organization?
  - What role/responsibilities do they have?
  - What access and authority do they have?
  - Who do they interact with (e.g., employees)?
- Personal:
  - What personal interests do they have?
  - What causes does they support?
  - What schools did they attend?
  - Who are their friends and relatives?
  - Where do they shop?

Probe for Points of Access or Entry

- Use common exploitation kits
- Identify entity's IP addresses and applications
- Find webmail or VPN
- Assess software versions in use
- Find outdated security patches
- Test for open network ports
- Scan for misconfigurations and outdated protocols

Attempt to Exploit Vulnerabilities

- Try out-of-the-box passwords and user names
- Perform brute force penetration attempts
- Send commands to system and wait for response
- Transmit payloads to target
- Leverage social engineering to dupe employees

SOCIAL ENGINEERING:

*The art of capitalizing on **relationships** and **social behavior** to **manipulate** people into providing access, supplying information or performing an action.*

Business Email Compromise

- Uses legitimate email accounts that were compromised
- Emails looks very real, and may sometimes have CEO's or senior exec's signature
- Targets lower-level staff that have access to company bank accounts or sensitive data
- Will also attack someone in the payroll department to try and steal payroll files
- Emails usually convey a sense of urgency

FBI: Global Business Email Compromise Losses Hit $12.5 Billion – July 16, 2018

'CEO Fraud' Remains Alive, Well and Underreported

Source: https://nachalegacy.nacha.org/content/business-email-compromise-vendor-impersonation-fraud-and-payments-what-organizations-and.

Example of Business Email Compromise

From: Alex Smith <asmith@cjpia.org>
Sent: Monday, June 17, 2019 10:32 AM
To: Grazyna Buchowiecki <gbuchowiecki@cjpia.org>
Subject: Request to Transfer Funds for an Investment Program

Hi Grazyna,

Jon has requested a transfer of $745,000 USD to be processed to the attached wire instructions today, I spoke to Jon over the phone about this payment already.
Can you get this processed right away?

Thank you,
Alex

Example of Business Email Compromise

From: Jonathan Shull
Sent: Monday, June 17, 2019 9:01 AM
To: Alex Smith
Subject: Request to Transfer Funds for an Investment Program

Hi Alex,

Per our discussed, Please find attached wiring instruction for payment

Thank you,
Jon

JONATHAN R. SHULL, CHIEF EXECUTIVE OFFICER
CALIFORNIA JOINT POWERS INSURANCE AUTHORITY
8081 MOODY STREET
LA PALMA, CA 90623

OFFICE: 562-467-8717
MOBILE: 562-897-8717
EMAIL: JSHULL@CJPIA.ORG

BANORTE

TO WHOM IT MAY CONCERN

This letter is to advise in writing the wire transfer information for your **Banco Mercantil del Norte (Banorte)** account.
The following information is being provided to you our customer; **FIN INVESTMENTS S.A** for the purpose of wire transfers.

WIRING INSTRUCTION;

- BANK NAME: BANCO MERCANTIL DEL NORTE (BANORTE BANK)
- BANK ADDRESS: AVENUE REVOLUCION 3000, PRIMAVERA, MONTERREY, NL 64830

- ACCOUNT NAME: FIN INVESTMENTS S.A
- BENEFICIARY ADDRESS: MADERO # 190 OTE, CENTRO MONTERREY, NL 64000

- ACCOUNT NUMBER: 072-225-003-559-148-838
- SWIFT CODE: MENOMXMTXXX

Please note: It is very important that you identify the correct account number and SWIFT code where applicable.

We value your business. Please call me if you have any further questions.

Regards,

Martinez Jorgé
Client Service Sr. Associate
Senior Relationship Manager

Example of Business Email Compromise

From: Grazyna Buchowiecki
Sent: Monday, June 17, 2019 1:16:25 PM
To: Alex Smith; Jonathan Shull
Subject: FW: Request to Transfer Funds for an Investment Program

Is this legitimate or is it a scam?

From: Alex Smith <asmith@cjpia.org>
Sent: Monday, June 17, 2019 11:29 AM
To: Grazyna Buchowiecki <gbuchowiecki@cjpia.org>; Jonathan Shull <jshull@cjpia.org>
Subject: Re: Request to Transfer Funds for an Investment Program

Grazyna, It is legitimate. Please proceed with payment.

Example of Business Email Compromise

From: Grazyna Buchowiecki
Sent: Monday, June 17, 2019 1:35:33 PM
To: Alex Smith
Subject: RE: Request to Transfer Funds for an Investment Program

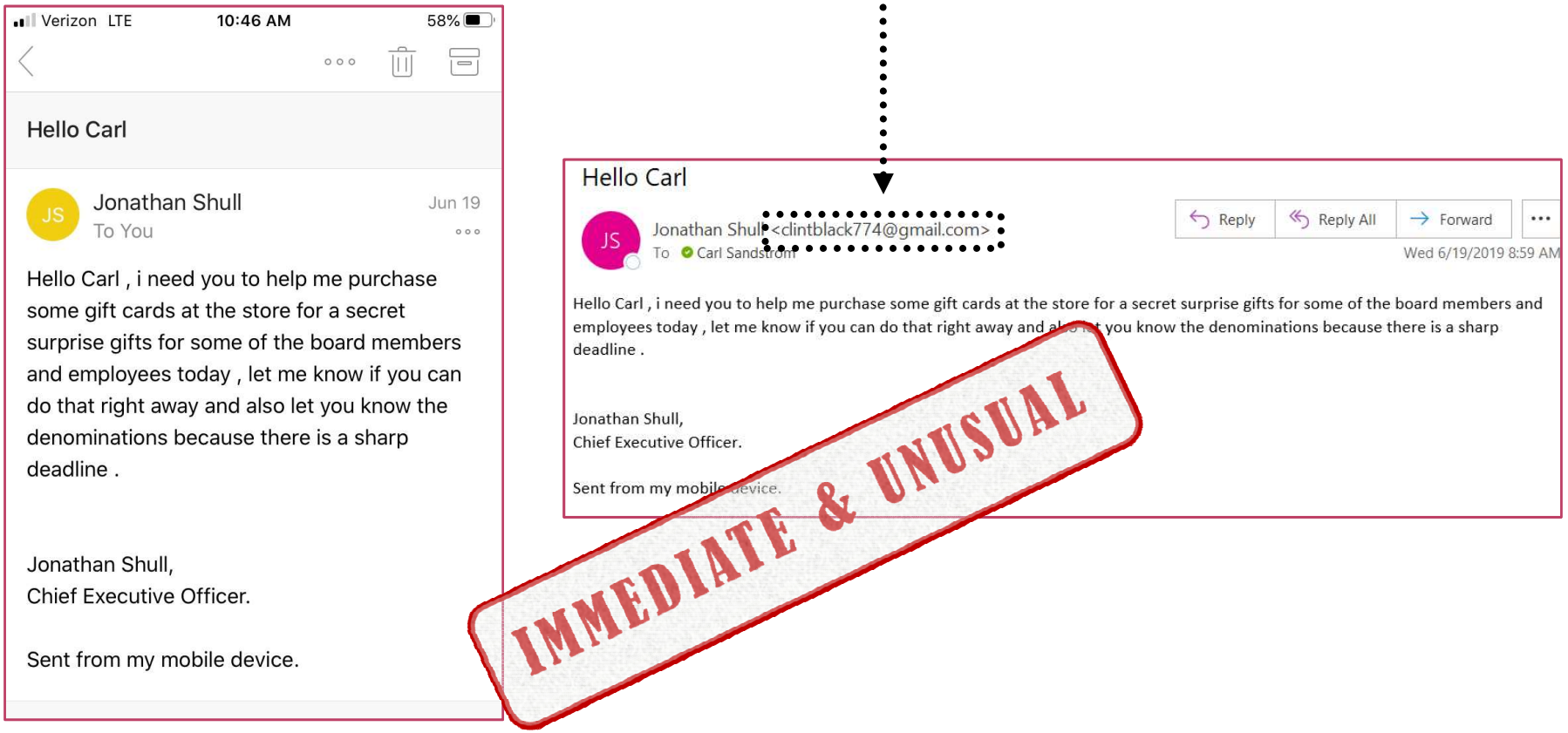
Alex,

I don't feel secure to do this wire. You want me to transfer money to Mexico.

From: Alex Smith <asmith@cjpia.org>
Sent: Monday, June 17, 2019 11:43 AM
To: Grazyna Buchowiecki <gbuchowiecki@cjpia.org>
Subject: Re: Request to Transfer Funds for an Investment Program

Grazyna, The request came from Jon, and I have spoken to him concerning the wire, So please proceed with the payment and let me know when it is done.

Gift Card Scam



What You Can Do: Impersonation Attacks

- ✓ **Train all employees!**
- ✓ Authenticate requests to make payments or change payment information.
- ✓ Make change requests to profiles and authorized personnel via secure website.
- ✓ Implement and follow strict protocols that require verification of a requestor of a wire transfer via telephone or in person.
- ✓ Initiate payment using dual control – require two people to approve payment initiation or make changes to payments.
- ✓ Review your accounts frequently for unusual activity.
- ✓ Never provide user credentials or sensitive account information via email or phone.
- ✓ Leverage multi-factor authentication (MFA) to help protect your network, business application and email credentials.

Audience Participation: Is this email real?

From: An NGUYEN <An.NGUYEN@gihs.sa.edu.au>
Sent: Wednesday, December 18, 2019 4:54 PM
To: IT_Admin@webmaster.com
Subject: Caution on Your Current Mailbox Storage Usage
Importance: High

We noticed that your Mailbox allocated storage is almost at Its limit.

90% 100%

Current Storage Usage.

You might be currently experiencing some defects in your Mailbox like;

- Delay in receiving messages
- Delay in sending messages
- Delay in forwarding messages
- Delay in creating reminders

Due to Your current storage Usage.

At 100% Storage Usage, When your allocated storage Capacity is used up to the limit you will experience more defects like, Inability to Use Certain email features like;

- Sending messages
- Receiving messages
- Forwarding messages

If you Have or Haven't started to experience the above Mailbox defect we suggest you visit the Web Storage Access page and login to automatically send a request to your Mailbox Administrator to adjust and maintain your storage now.

NOTE: The Web Storage Access Login page was created to allow users login with their Mailbox credentials and automatically send request to your Mailbox Administrator to adjust and maintain your Mailbox storage, If your Login was successfully Authenticated. But your request will not be sent if your login credentials were not authenticated due to incorrect credentials.

IT Help Desk Admin
(An NGUYEN)
Office of Information Technology

This message is intended for the addressee named and may contain privileged information or confidential information or both. If you are not the intended recipient please delete it and notify the sender.

Vendor Impersonation Fraud

The fraudster:

- ✓ Impersonates a legitimate vendor or contractor.
- ✓ Creates an email address that is similar to the actual email address, making it difficult to spot. Written correspondence may appear to be on legitimate letterhead or stationery.
- ✓ Contacts businesses or public-sector entities by telephone, email, snail mail or fax.
- ✓ Requests that account information for payment be changed to an account controlled by the fraudster. When an invoice is received, the entity processes a payment to the fraudster.

Vendor Impersonation Fraud

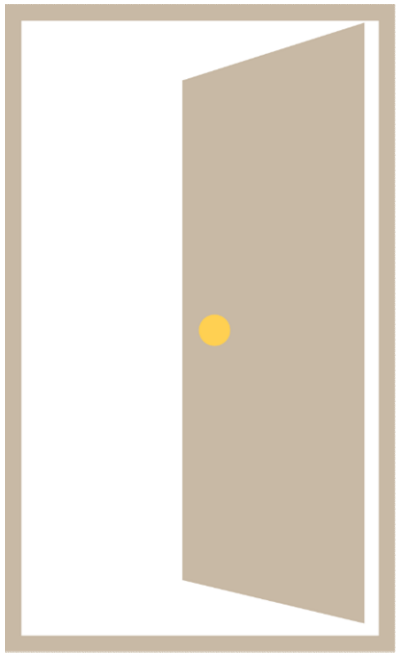
Public-sector entities are often targeted because their contracting information is typically a ***matter of public record****.*

County lost $1.7 million in email scam – July 31, 2019

Scammers posed as the firm hired as the general contractor for a new high school.

Source: https://statescoop.com/north-carolina-cabarrus-county-lost-1-7-million-email-scam/

Tailgating



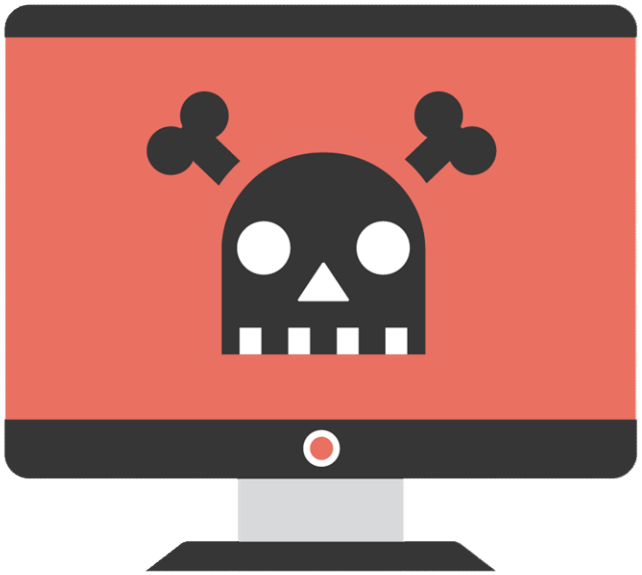
- Attacker takes advantage of holding a door open to compromise physical security of a location

Risks:

- Access to passwords on sticky notes
- Computer login attempts
- Access to physical files/documents that could be used for later breach or compromise
- Ability to plug computers into network jacks or access Wi-Fi and deploy malware on network

Once They're In…

- **Network Infiltration**
  - Malware
  - Key logger
  - Ransomware
- **Persistence on the network**
  - Malware lays dormant, then spreads
  - Lateral movement
  - Escalation of privileges



Once They're In…

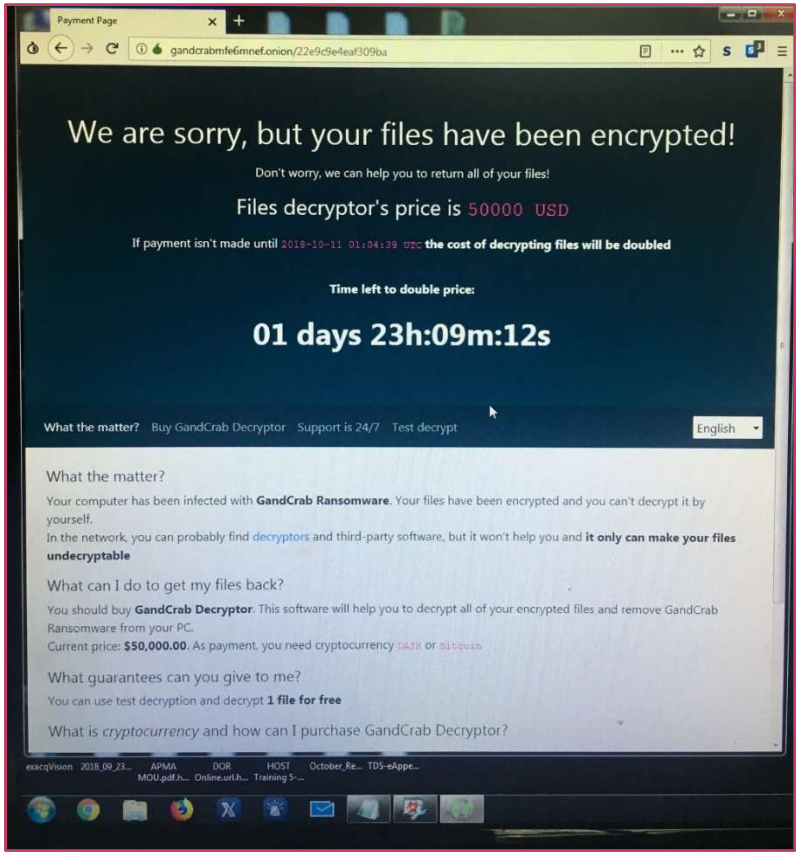
- **Do damage or harm!**
- **Obfuscation/exfiltration**
  - Erase all evidence and exit

Ransomware

- Ransomware is a type of malicious software that infects, locks or takes control of a system, or encrypts important data and demands ransom to undo it.
- Typically installed through a malicious email attachment, an infected software download or visiting a malicious website.
- Payment requests are made in bitcoins, wire services or gift cards, which are hard to trace.
- Some ransomware will act like a worm and spread throughout network onto other computers without interaction by the attacker.

Example of Ransomware

Ransomware has been used against local governments, preventing the delivery of ***critical services***.



What You Can Do: Ransomware

- ✓ **Train all employees!**
- ✓ Know where your critical data resides (crown jewels) and take extra precautions for it.
- ✓ Make sure your data is being backed up and can be restored successfully – test and verify!
- ✓ Talk with your IT department about:
  - Tools they have in place
  - Frequency of software patch updates
  - Technical controls and procedures they employ
  - What they would do in the event of an attack

Audience Poll:

Are you allowed to install software
on your computer?

What Cybersecurity Threats Could Cost

- Average cost of a data breach - **$3.86 million**
- The cost of lost business after a data breach - **$4.2 million**
- Notification cost after a data breach - **$740,000**
- Average time to contain a data breach - **69 days**

- Global cost of online crime is projected to be **$6 trillion** by 2021
- Attacks are growing by more than **350%** annually

Sources: 2018 Data Breach Investigations Report 11th Edition.

Things to Tell Your Board or Council

Rising tides lift all boats…

As the use of digital technologies create huge business and consumer benefits, their use also advances the capabilities of cyber criminals.

> Cyber attacks are currently considered among the top three risks to global security.

- ✓ Breaches are harder to detect than ever before.
- ✓ The public sector is at high risk and the performance of critical services is at stake.
- ✓ Employee training and awareness is your #1 defense.

Best Practices for Cybersecurity

- ✓ **Train all employees!**
- ✓ Follow an Information Security Program that includes strong password requirements, account lockouts, an Incident Response Plan, and other cybersecurity measures.
- ✓ Use a strict Data Security Policy with industry standard encryption of data both in transit and at rest. Only authorized users who have a business need for it should have access to your data.
- ✓ Adhere to industry standards for network and systems security. This includes managing all software and keeping it up-to-date.
- ✓ Use independent third-parties to perform penetration tests and vulnerability assessments to identify security risks and other weakness that expose an organization to a cyberattack.

Resources for Your IT Professionals

- ✓ California County Information Services Directors Association (CCISDA)
  https://www.ccisda.org/

- ✓ California Consumer Privacy Act Law
  https://www.oag.ca.gov/privacy/ccpa

- ✓ Municipal Information Systems Association of California
  https://www.misac.org/

Questions Welcome

If you have additional questions, please email them to bensonk@pfm.com and csandstrom@cjpia.org.

Thank you for joining us today!

About the Presenters

Kerry Benson, PFM

Managing Director & Chief Information Officer

Kerry Benson serves as managing director and chief information officer for PFM. He is responsible for overseeing all firm-wide information technology (IT) activities and resources, including infrastructure management, telecommunications and networks, system security plans, facilities, business continuity and disaster recovery applications development, project management, business process reengineering, outsourcing, marketing support and auxiliary operations. He chairs the PFM Technology Committee, which plays an active role in shaping the firm's long-term technology strategy.

Carl Sandstrom, California JPIA

Business Projects Manager

Prior to joining the California JPIA, Carl worked in the field of risk management in the finance industry for 17 years. He has been a valuable member of the California JPIA's team since 2003. Carl holds a bachelor's degree in Economics from San Diego State University and the Associate in Risk Management - Public Entities designation. He is currently the California JPIA's Business Projects Manager and is responsible for various information technology and communications projects. Carl is a member of the California Association of Joint Powers Authorities (CAJPA) Technology subcommittee.

Important Disclosures

This material is based on information obtained from sources generally believed to be reliable and available to the public, however PFM's Asset Management business cannot guarantee its accuracy, completeness or suitability. This material is for general information purposes only and is not intended to provide specific advice or a specific recommendation. All statements as to what will or may happen under certain circumstances are based on assumptions, some but not all of which are noted in the presentation. Assumptions may or may not be proven correct as actual events occur, and results may depend on events outside of your or our control. Changes in assumptions may have a material effect on results. Past performance does not necessarily reflect and is not a guaranty of future results. The information contained in this presentation is not an offer to purchase or sell any securities.