Cybercrime and Identity Theft: Awareness and Protection
2015 HLC Conference

Christopher T. Van Marter
Senior Deputy Prosecuting Attorney
Chief – White Collar Crime Unit
Department of the Prosecuting Attorney
1060 Richards Street
Honolulu, Hawaii 96813
Ph: 808-768-7436
Fax: 808-768-7513
E-mail: cvanmarter@honolulu.gov
Cybercrime Statistics

- In 2014, the New York Times devoted more than 700 articles to stories about “data breaches” compared to just 125 in 2013
- A record 1 billion data records were compromised in 2014
- Notable 2014 Victims:
  - Sony
  - Blue Cross
  - Anthem
  - Home Depot
  - Staples
  - JP Morgan Chase
  - Target (December 2013)

Gemalto, Findings of 2014 Breach Level Index, Feb. 12, 2015
Cybercrime Statistics

- In 2014, the number of detected cybercrime incidents soared to 42.8 million, a 48% increase from 2013.
- Since 2009, the number of detected cyber incidents rose 66%.
- The costs associated with those incidents also continues to rise.

*PWC 2015 US State of Cybercrime Survey*
I3C Cybercrime Statistics

- In 2014, there were 269,422 complaints filed with the Internet Crime Complaint Center (I3C)
- The total reported losses were $800,492,073
- The average loss was $6,472
- 91% of the victims were US citizens
- According to the Department of Justice and the I3C, less than 10% of fraud victims file a report
Hawaii Cybercrime Statistics

- In 2014, Hawaii ranked 40th in the country in terms of the number of victims
- 1,020 Hawaii victims filed a complaint
- Those 1,020 victims reported losses of $2,497,141
- In addition to complaints being filed with the I3C, complaints are also filed directly with HPD
Threat Awareness
Threat Awareness

Two types of threats:

- Internal threats
- External threats
Internal Threats

- Current and former employees
- Insider threat cases account for only about 20% of the reported cases
- Insider threat cases are under reported
  - Why?
    - “Handled it administratively”
    - “Not serious enough”
    - “Didn’t know it could be prosecuted”
    - “Negative publicity”
- Insider threat cases represent about 60% of the cases prosecuted
Internal Threats – Crimes?

- Intellectual property theft
- IT sabotage
- Denial of service attack
- Fraud
- Unintended insider threats

Insider threat motives:
- The perpetrator’s motive is usually financial gain or revenge
- Many of the perpetrators were experiencing financial difficulties at the time
Internal Threat Actors

- 5734K12: CARELESS USER
- 8813D4: PAYMENT CARD BREACH
- 3287MB: INDUSTRIAL ESPIONAGE
- 6635RB: DATA THEFT
- 9151P4: I.T SABOTAGE
External Threats

- Individuals not known to the victim
- Represent about 80% of the reported cases
- External Threat Actors:
  - Hackers
  - Con artists
- External threat motive:
  - Usually, for financial gain
- Prosecution is unlikely if the actor is located outside the United States
External Threat Actors

70% of the perpetrators are located overseas
External Threats to Businesses
Ransomware Threats

- Ransomware = malicious software designed to extort money from individuals and/or businesses by disabling important computer functions and by encrypting critical files.
- Encrypted files become irretrievable unless the victim buys a decryption key.
- Criminals demand a ransom payment in exchange for the decryption key.
- No guarantee criminal will honor their promise to provide the decryption key upon payment.
Cryptolocker

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Ransomware

- Common attack vectors:
  - **E-mail** which, if opened, will install ransomware
  - **E-mails that contain links** which, if clicked, will install ransomware
  - **E-mail that contain attachments** which, if clicked, will install ransomware

- Ransomware may encrypt documents, images, videos, and other important files
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [???]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [???] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
YOUR COMPUTER HAS BEEN LOCKED!

Your computer has been locked due to suspicion of illegal content downloading and distribution.

The illegal content (414 MB of photo and video files) was automatically classified as child pornographic materials.

The downloading and distribution of illegal content, in whole or in part, violate the U.S. Federal Laws:
- 18 U.S.C. § 2251 Sexual exploitation of children (Production of child pornography)
- 18 U.S.C. § 2252aCerul activities relating to material involving the sexual exploitation of minors (Possession, distribution, and receipt of child pornography)
- 18 U.S.C. § 2252bCerul activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 6 months to 10 years and shall be fined up to $250,000.

Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) §512.

Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300

Your IP address: [redacted]
Your host name: [redacted]
Source or intermediary sites: [redacted]
Location: [redacted]

Illegal content found:

[Images of alleged illegal content]

Exchange your cash for a MoneyPak voucher and use your voucher code in the form below:

Code: [input fields]
Status: Waiting for payment
Permanent lock on 09/28/2013 8:46 p.m. EST

Where can I buy MoneyPak:
- Rite Aid
- CVS
- Kmart
- 7-Eleven
- Walgreens
- Walmart
Your computer has been locked due to suspicion of illegal content downloading and distribution. Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2252 - Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A - Certain activities relating to material constituting or containing child pornography.

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
- Involved IP address: [redacted]
- Involved host name: [redacted]
- Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don’t try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U.S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

Permanent lock on 05/01/2013 5:20 p.m. EST
Ransomware

- Common attack vectors:
  - E-mail which, if opened, will install ransomware
  - E-mails that contain links which, if clicked, will install ransomware
  - E-mail that contain attachments which, if clicked, will install ransomware

- Ransomware may encrypt documents, images, videos, and other important files

- Victims are more likely to recover from a ransomware attack if they regularly backup their critical data
Spearphishing

- Spearphishing attacks target specific individuals, as opposed to phishing schemes which target hundreds and sometimes thousands of people.
- They victimize only those who open e-mails or click on attachments or links.
- Spearphishing e-mails are written to create the impression that you know or do business with the sender.
ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/smartphone/network.

9. The hacker uses the backdoor to steal information.
Join my network on LinkedIn

LinkedIn

[Name] has indicated you are a Friend:

I'd like to add you to my professional network on LinkedIn.

Accept

DID YOU KNOW you can use your LinkedIn profile as your website?
Select a vanity URL and then promote this address on your business cards, email signatures, website, etc.

© 2011, LinkedIn Corporation
Bogus Anti-Virus Software

1. A pop-up box appears that informs the user that their computer is infected with a virus and needs to be fixed
2. The pop-up box has a button that the user can click to download anti-virus software that will remove the virus
3. The user clicks on the button thinking that it will help
4. Instead, the user’s computer is infected with malware, which steals personal and financial information
Employment E-Mails

1. The perpetrator sends an e-mail to an employer in response to an online job posting.
2. The e-mail contains an attachment, which the perpetrator claims is a resume.
3. When the employer clicks on the attachment, malware is downloaded and used to steal personal information.
Dear Sir,

I would like to apply for the job you have advertised on Craig's List. Attached is my resume and portfolio.

Regards,
Marshall Mac
Employment E-Mails

1. The perpetrator sends you an e-mail claiming that they saw your resume on CareerBuilder or Monster, or the Internet.
2. They tell you that you’re the perfect candidate for an opening with their company.
3. They want to hire you now!
4. All they need you to do is complete the attached application, then send them your credit report so they can verify your credit history and your bank account information so they can make direct payroll deposits to your bank account.
Dear Sirs,
The Better Business Bureau has got the above-referenced complaint from one of your associates on the subject of their dealings with you. The detailed information about the consumer's concern is presented in enclosed file. Please examine this case and inform us about your opinion. Please click here to reply this complaint.

We look forward to your prompt response.

Yours faithfully,
Shawna Dennis
Better Business Bureau
November 08, 2011
Re: 000012-91273771

Dear, John
Thank you for your request for a credit report. Please find it in the attachment.

* If you feel you have additional information you wish to submit to us that might influence our decision, feel free to write to us at the address listed at the bottom of this letter. Please include the reference number on any correspondence.

Equifax Corporation
P.O. Box 740241
Atlanta GA 75013-0036
1-800-685-1111
You sent an automatic payment.  

Hello Member,

You sent an automatic payment to Dedicated Servers. Here are the details:

<table>
<thead>
<tr>
<th>Amount:</th>
<th>$90.00 USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>For:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dedicated Servers monthly recurring subscription for $90.00 per year for Dedicated Servers, including 30-days money back guarantee. Cancel any time.</td>
</tr>
</tbody>
</table>

Do you confirm this payment?

If this payment was not made by you please immediately take the following steps:

* Login to your account by clicking on the link below:
* Provide requested information to ensure you are the owner of the account
* Find this transaction in HISTORY and click 'Cancel Transaction'

CANCEL TRANSACTION

Please don't reply to this email. It'll just confuse the computer that sent it and you won't get a response.

PayPal Email ID PP1204
Fraudulent Tech Support Calls

1. An employee receives a phone call from a person claiming to be “tech support” for a legitimate company (such as Dell, Microsoft, Apple, etc.)

2. Tech Support then asks for log-in credentials or asks the employee to make changes to the computer’s settings, or asks the employee to visit a specified website and download various files to give Tech Support remote access to the computer so they can fix the problem.

3. Sometimes, Tech Support asks the employee to turn off the monitor so they don’t interfere with the fix.

4. Tech Support then steals information.
“HI, I’M CALLING YOU FROM MICROSOFT TECH SUPPORT”
You may think the caller is a friendly representative from Microsoft’s Tech Support...........
but think again.

Tech Support Scams are Happening.
Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

⚠️ High Importance

Please process a wire transfer payment in the amount of $250,000 and code to “admin expenses” by COB today. Wiring instructions below...

Business E-Mail Compromise
An Emerging Global Threat
Business E-Mail Compromise aka “CEO Fraud”

1. These are targeted spearphishing scams
2. These scams typically target the CEO or other high-ranking company official
3. The perpetrator begins by researching the target and target’s employer
4. High-ranking officials and those responsible for handling wire transfers and online payments are targeted
Business E-Mail Compromise aka “CEO Fraud”

- Between October 2013 and August 2015, more than 7,000 companies were the victim of “CEO Fraud”
- Those companies reported losses of nearly $750 million
- The scam was reported in all 50 states and in 79 countries
- The majority of the money is being wired to Asian banks in Hong Kong and China
Version 1:

The e-mail account of the CEO or other high-ranking official is compromised by either a phishing e-mail scheme or by hacking.

Then, the perpetrator uses the compromised e-mail account to send an e-mail to a second employee who handles financial transactions.

The e-mail requests that a wire transfer or online payment be directly made to company “X’s” financial institution.

The e-mail is usually well-worded, includes a “sense of urgency” clause, and is in an amount similar to normal business transaction amounts for that company.
Business E-Mail Compromise aka “CEO Fraud”

Version 2:

- The perpetrator identifies the company employee responsible for handling financial transactions
- Then, that employee’s e-mail account is compromised, typically by phishing or hacking
- The perpetrator then sends e-mails to multiple vendors used by that company
- The vendors are identified by reviewing the compromised account’s contact list or e-mails
- The e-mails to the vendors request invoice payments in the form of wire payments or online transfers, which go to a fraudulent account controlled by the perpetrator
Business E-Mail Compromise aka “CEO Fraud”

Version 3:

- The perpetrator learns that company X has a long-standing relationship with supplier Y.
- The perpetrator creates a fictitious e-mail address which looks similar to the domain name used by the supplier.
  - For example: @examp1e.com instead of @example.com
- The perpetrator sends an e-mail to the employee responsible for handling financial transactions.
- The e-mail includes an invoice to company X requesting payment in the form of a wire transfer or online payment, which goes to an account controlled by the perpetrator.
Wi-Fi Attacks
Wi-Fi Attacks
Wi-Fi Attacks
Wi-Fi Attacks
Wi-Fi Attacks

- Favorite targets: hotels, airports, Internet cafes
- How it works: Hackers set up a fake Wi-Fi network
- They give the network a name like “Free Wi-Fi” or a name that is similar to the victim’s location
- When victims use their device to search for a Wi-Fi connection, they see the fake Wi-Fi network
- They connect to the network
- Then, start surfing the Internet
- The only problem, all of their communications are going through the hacker’s computer
- Besides intercepting all of the communications, the hacker can also steal passwords, financial data, and other confidential information
Internet of Things (IoT) Risks

- IoT – refers to any device which connects to the Internet to automatically send and/or receive data

- IoT examples: Devices which control:
  - Lighting systems
  - Security systems
  - Thermostats
  - Garage doors
  - “Smart appliances”
  - Entertainment devices
  - Office equipment, such as printers
  - Medical devices
Internet of Things (IoT) Risks

- Exploitation of default IoT passwords
- Steal confidential and personal information
- Remotely monitor the owner
- Overload a device to render it inoperable
- Compromising the IoT device to cause physical harm

Protection:
- Change default passwords to strong passwords
- When available, update IoT devices with security patches
Protecting Financial & Personal Information:
Checklist for Businesses

- Identify the types of information that you collect, store, or transmit
  - Names, addresses, phone numbers, e-mail addresses
  - SSN’s, DOB’s, HDL’s
  - Payment card information, account numbers, and transactional information

- Minimize what you collect, store, and transmit

- Destroy information when it's no longer needed
Checklist for Businesses

 Identify **how** you store your information
  • Hardcopy paper records
  • Electronic files

 Identify **where** your information is stored
  • Desk drawers
  • Filing cabinets
  • The mail room
  • A home office
  • Electronic devices – desktop/laptop computers, tablets, servers, cellular phones, external storage drives, remote or cloud storage services
Checklist for Businesses

- Identify who has access to your information
  - Limit access to those employees with a need to know
  - Does the information leave the office?
    - In the form of hardcopy records?
    - On mobile devices?
  - Limit remote access to the information
Checklist for Businesses

- **Password-protect storage devices**
  - Never use default password
  - Use “strong” passwords (letters, numbers, symbols)
  - Change passwords frequently (every 90 days)

- **Block unauthorized access**
  - Use a firewall
  - Update the operating system and antivirus software
  - Use encryption
  - Perform routine scans of your systems for malware

- **Backup critical data**

- **Employee awareness training**
Checklist for Businesses

- Regularly monitor networks/systems that contain card payment data
- Assign a unique username and password to each employee who accesses financial data
- Encrypt card payment data transmitted via wireless or public networks
- Use payment compliant software and systems
- Do not store magnetic strip and security code information after authorization
- Do not store unencrypted cardholder data
- Do not leave remote applications in “always on” mode
- Do not use default vendor-supplied passwords
Checklist for Businesses

- Destruction of personal information
  - Do NOT simply move files to the “Recycler” folder
  - Do NOT simply “delete” files
  - Use data wiping software
  - Use specialized shredders on CD’s & DVD’s disks
  - Consider using a certified disposal company

- Do not share information about your computer systems or information security practices
Checklist for Individuals

➢ The Rule: Never disclose personal information over the phone, through the mail, or over the Internet unless you initiated the contact and you trust the person or company that you’re dealing with

• Ask yourself: Who contacted who?
• If a person or company contacts you, do NOT disclose any personal information to that person or company – period!
  o Do not open e-mails; do not click on links; do not click on attachments; end the phone call
  o Then, contact the company directly through their KNOWN website or phone number
Checklist for Individuals

• If you receive an e-mail or message asking for personal information, do NOT open it or click on any link or attachment to it.

• If you’re not sure whether the request is legitimate, contact the company directly in a way you know to be genuine, for example, calling the number listed in the phone book or on the company’s legitimate website.
Checklist for Individuals

• Use your operating system’s firewall
• Consider using a hardware firewall system
• Update antivirus software regularly
• Update your operating software regularly
• Secure your passwords
• Backup important files
Data Breach

- Create a data breach notification policy
- Train your employees to spot a data breach
- Immediately gather the facts
- Notify financial institutions
- Notify affected customers
- Notify law enforcement
Wi-Fi Security

➢ Turn off “sharing” - file, printing, network, and public folder sharing

➢ Enable your device’s firewall

➢ Use https:// whenever possible
  • Encrypted websites

➢ Use a VPN - Virtual Private Network (Examples: Cyberghost, OpenDNS)

➢ Turn off Wi-Fi when you’re not using it
Wi-Fi Security

- Consider using your cell phone as a Wi-Fi hotspot
- Disable automatic network connections
- Do not conduct financial transactions or online banking while travelling
- Protect your devices against the fallout from theft or loss:
  - Set a lockout passphrase
  - Set a short lockout time period
  - Enable remote wiping
  - Enable location tracking (Example: “Find My iPhone”)
- Consider using two-factor authentication for an online accounts
Wi-Fi Security

- Employers should require that employees use a corporate VPN and encryption when making connections and exchanging data
  - Corporate IT can setup a computer to automatically connect to a VPN and encrypt data
- Adopt corporate policies that prohibit employees from transferring sensitive data to mobile devices or unauthorized personal or home computers
- Provide employees with mobile Wi-Fi hotspots that use cellular connections
Hawaii’s Identity Theft Cybercrime Laws
Identity Theft

- A person commits the crime of identity theft if he uses the personal information of another with intent to commit theft
  - **First Degree** – loss exceeds $20,000
    - 20 year prison term
  - **Second Degree** – loss exceeds $300
    - Up to 10 year prison term
  - **Third Degree** – loss is less than $300
    - Up to 5 year prison term
A person commits the crime of computer fraud if he accesses a computer with intent to commit theft

- **First Degree** – loss exceeds $20,000
  - 20 year prison term
- **Second Degree** – loss exceeds $300
  - Up to 10 year prison term
- **Third Degree** – loss is less than $300
  - Up to 5 year prison term
A person commits the crime of unauthorized computer access if he knowingly accesses a computer, computer system, or computer network without authorization, and thereby obtains information, and:

- The offense is committed for private or commercial gain;
- The offense was committed in furtherance of any other crime;
- The information has been deemed confidential by law; or
- The value of the information obtained exceeds $20,000

20 year prison term
Computer Damage 1st

- A person commits the crime of computer damage if he causes damage to a computer, computer system, or computer network that manages or controls any critical infrastructure, and the damage results in the substantial impairment of:
  - The computer, computer system or computer network; or
  - The critical infrastructure managed or controlled by the computer, computer system, or computer network.

- 20 year prison term
Resources

- http://honoluluprosecutor.org/white-collar-crimes/
- http://www.idtheftcenter.org/
- http://www.consumer.ftc.gov/search/site/identity%20theft
Questions?

Christopher T. Van Marter
Senior Deputy Prosecuting Attorney
Chief – White Collar Crime Unit
Department of the Prosecuting Attorney
1060 Richards Street
Honolulu, Hawaii 96813
Ph: 808-768-7436
Fax: 808-768-7513
E-mail: cvanmarter@Honolulu.gov