BARRY CAPLIN
THE ACCIDENTAL INSIDER
WED. MAY 13, 2014, 1:30P
WELCOME TO SECURE360 2014

➤ Come see my talk tomorrow!

➤ The CISO Guide – How Do You Spell CISO? – Wed. 11A
The Accidental Insider

Secure360

Tues. May 13, 2014

bcaplin1@fairview.org
bc@bjb.org   @bcaplin

http://about.me/barrycaplin

http://securityandcoffee.blogspot.com

Barry Caplin
Chief Information Security Official
Fairview Health Services

http://about.me/barrycaplin
securityandcoffee.blogspot.com
@bcaplin
Fairview Overview

- Not-for-profit established in 1906
- Academic Health System since 1997 partnership with University of Minnesota
- >22K employees
- >3,300 aligned physicians
  - Employed, faculty, independent
- 7 hospitals/medical centers (>2,500 staffed beds)
- 40-plus primary care clinics
- 55-plus specialty clinics
- 47 senior housing locations
- 30-plus retail pharmacies

2012 data

- 5.7 million outpatient encounters
- 74,649 inpatient admissions
- $2.8 billion total assets
- $3.2 billion total revenue
Who is Fairview?

- Fairview Ridges Hospital
- Fairview Range Health Services
- Fairview Southdale Hospital
- Fairview Northland Medical Center
- Fairview Lakes Medical Center

University of Minnesota

Children’s Hospital

Medical Center

Ebenezer PreferredOne

Maple Grove Hospital

A partnership of North Memorial and Fairview

Columbia Park Medical Group

Part of Fairview

Institute of Athletic Medicine

Minnesota Sports Medicine
Ex-IRS Employee Sentenced for Identity Theft and Tax Fraud

NASHVILLE (AUGUST 24, 2012)
BY MICHAEL COHN

A former Internal Revenue Service employee has been sentenced to two years in prison for identity theft and filing fraudulent income tax returns.

Insider Case Exposes Security Lapses
Bank Manager Pleads Guilty to Theft

By Tracy Kitten, May 24, 2012. Follow Tracy @FraudBlogger

In Pennsylvania, a former PNC Bank branch manager pleaded guilty to bank theft - a charge that included stealing funds and using those funds for personal use.

Insider data theft costs Bank of America $10 million

By Robert McMillan
May 25, 2011 09:03 PM ET

IDG News Service - A Bank of America insider who sold customer data to criminals cost the bank at least US$10 million in losses.

State worker stole IDs for fraud

Article by: DAVID CHANEN and DAN BROWNING, Star Tribune staff writers
Updated: June 21, 2012 - 7:46 PM

Ring based in Minnesota allegedly used stolen identity data to defraud numerous banks and retailers.
In The News

LAPD officer resigns after being accused of tapping database on killer's behalf

Rookie sought information on key witnesses in the trial of a man whose sister he was dating, court documents say. Prosecutors will decide whether to file charges after an investigation is completed.

By Joel Rubin and Jessica Porter, Los Angeles Times
November 14, 2010 | 6:32 p.m.

A rookie Los Angeles police officer has resigned amid allegations he illegally tapped into a law enforcement computer on behalf of a gang member who was recently convicted of murder.

Former Sprint-Nextel employee sentenced for improper disclosure of phone records to cocaine dealer

November 24, 2010 by admin
Filed under Breach Incidents, Business Sector, Insider, U.S.

Amy Quesnel, 29, of Georgia, Vermont was sentenced yesterday to six months imprisonment to be followed by four months of supervised detention.
The defendant’s charge was included in a twenty-count/twenty defendant Indictment that alleges that Michael Olsen, 36, of Vermont had participated in a large cocaine conspiracy in northwestern Vermont. The Indictment alleges that Olsen owned Rizzo Bros. automobile deal on Commerce Avenue in South Burlington but operated it as a front for a multi-kilogram cocaine distribution organization.
The Indictment alleges that Olsen directed others, including codefendant Andrew Bullock, 29, of Essex Junction, to mail large amounts of cash (usually over $20,000) to cocaine suppliers in California and Arizona. The Government charges that kilogram[s] of cocaine were sent to the suppliers, then be sent to third party addresses in Chittenden and Franklin Counties where other coconspirators would pick it up and sell it to local drug traffickers.
Briefing Note: Operation PATHWAY

- General overview
  This is a Security service led investigation into suspected AQ driven attack planning within the UK.

The current Executive Action phase relates to:

11 subjects addressed:
- GMP
  - Dynamic entry - firearms
  - Merseyside
  - Dynamic entry - firearms
  - Lancashire
  - Unarmed entry due to the premises being of Bed & accommodation type

- Immigration status
  10x student visa Pakistan born nationals - all from the UK born British national

- Planned detention
  Manchester 

  [Redacted]

- Command structures
  Investigation
  [Redacted]

- Command structures - GOLD
  GOLD GMP - Merseyside - GOLD - Lancashire

- Community Impact Engagement Reassurance
  Planned through Community GMP Plan to be ratified at GOLD meeting at 1300

- Media strategy
  Media strategy has been ratified and is being deployed.
Amazon blames human error for Xmas Eve outage; Netflix vows better resiliency

by Derrick Harris  DEC. 31, 2012 - 3:58 PM PDT

Power outage conspiracy theories take central stage in Super Bowl XLVII
A power outage appeared to alter the course of Super Bowl XLVII when the 49ers rallied against the Ravens. But was it an accident? A cunning plan by the broadcaster? Divine intervention? Beyoncé?

Pakistan causes YouTube outage for two-thirds of world

By Peter Svensson
NEW YORK

Most of the world's Internet users lost access to YouTube hours Sunday after an attempt by Pakistan's government domestically affected other countries.

Sprint blames major network outage on 'accidental dual fibercut'

Google Accidentally Transmits Self-Destruct Code to Army of Chrome Browsers
BY ROBERT MCMILLAN  12.11.12  6:30 AM

Wikipedia blackout after server cables accidentally cut
Online encyclopedia brought down for two hours after someone cut through cables connecting its servers in Florida
Agenda

• What is it?
• How big an issue?
• What do we do?
Internal Risk Management v Insider Threat
What is Internal Risk Management?

• Malicious Insider = Current or former staff who:
  – intentionally exceeded/misused authorized access to networks, systems or data, and;
  – affected security of organizations’ data, systems, or daily operations

• Insider’s intentions can be good or evil
• Actions can be intentional or accidental
• Must consider errors and omissions
  – Accidents
  – Not following process

(CERT/US Secret Service Insider Threat Study)
CSI/FBI Computer Crime Survey

• Not a new issue
• 2007 – Insiders #1 reported problem.
• 2008 – Insider threat decreased
• 2009 – Some attributed 60-100% of losses to accidents
• 2010/2011 –
  ➢ 40% attributed some loss to malicious insiders
  ➢ 60% attributed some loss to non-malicious insiders (accidents)
Verizon DBIR (Data Breach Investigations Report)

- 2008 & 2009 (based on Verizon-only)
  - Most = external, most costly = internal; 39% multiple parties
  - Didn’t consider insiders’ “inaction”
- 2010 (included US Secret Service)
  - Most = external, internal 48% (up 26%)
- 2011
  - Most external; 17% internal (-31%); 9% multiple parties
  - Simple; targets of opportunity; avoidable; most found by 3rd party
- But doesn’t consider accidents
2012 Verizon Breach Report

2012 report (included US Secret Service)

• Most = “external”; “internal” greatly decreased
• 79% of victims targets of opportunity
• 96% of attacks considered not highly difficult
• 96% of victims subject to PCI not compliant
• 97% were avoidable through simple or intermediate controls
## Unintentionally Exposed Data Still Just As Gone

In general, which of the following threats do you consider the most potentially damaging to your business?

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees/business partners unintentionally damaging or exposing business data</td>
<td>37%</td>
</tr>
<tr>
<td>Loss/theft of laptop/portable storage device</td>
<td>35%</td>
</tr>
<tr>
<td>Trojan horses</td>
<td>34%</td>
</tr>
<tr>
<td>Viruses/worms</td>
<td>32%</td>
</tr>
<tr>
<td>External attackers gaining unauthorized access to my company’s databases</td>
<td>20%</td>
</tr>
<tr>
<td>IT employees misusing their access privileges</td>
<td>18%</td>
</tr>
<tr>
<td>Phishing/pharming</td>
<td>18%</td>
</tr>
<tr>
<td>Employees/business partners stealing or sabotaging business data</td>
<td>18%</td>
</tr>
</tbody>
</table>
OK: Hundreds of personal documents found in dumpster

December 5, 2010 by admin

Filed under Breach Incidents, Business Sector, Exposure, Financial Sector, Paper, Subcontractor, U.S.

A Tulsa business finds hundreds of documents in its dumpster.

[...]

The documents contained all sorts of personal information, dating as far back as 2004 and as early as 2009. Probst managed to save 96 of them before sanitation workers came by and emptied the dumpster.

“Blank checks, social security cards, id’s, bank statements, telephone statements, everything. I mean it’s, it’s quite extensive,” Probst said.

The documents were traced back to a business a couple of doors down from probst called American Check Cashers of Oklahoma, LLC.
34% of resold hard drives contain personal data, study reveals

Researchers from BT and the University of Glamorgan are in the news today because they have found a disturbing number of hard drives sold on auction websites and at computer fairs contain sensitive information.

The study, conducted in the UK, United States, Germany, France and Australia, uncovered that 34% of the randomly purchased 300 drives contained personal data, including bank account and medical information that could be exploited for the purposes of identity theft.

In addition, details of test launch procedures for a ground-to-air missile defence system was found on a disk purchased on eBay.

We've discussed before the problem of people selling on used hardware like disk drives without properly wiping it. Last August, for instance, we revealed how details of bank customers was found on a hard drive sold on eBay for £35.

With sensitive data like this regularly resurfacing on used hard disks, I wouldn't be surprised if old clapped out hard drives have a higher monetary value than brand spanking new ones. :(

If the data on your hard drive was properly encrypted, of course, then you wouldn't need to worry about what happens next to your hardware - because the identity thief wouldn't be able to detangle the gobbledygook.

Don't make it easy for the criminals. If you're dumping old hardware, make sure you dispose of it appropriately and ensure that any data contained on the drives is either securely wiped or was strongly encrypted in the first place.

Posted on May 7th, 2009 by Graham Cluley, Sophos
Types of Internal Risks

- **Fraud**: obtaining property or services through deception or trickery.
- **Theft of Information**: stealing confidential or proprietary information.
- **IT Sabotage**: acting with intent to harm an individual, organization, or organization’s data, systems, operations.
- **Error/Omission**: causing damage to assets or disclosure of information because of an unintentional mistake.
  - Leaving a system vulnerable (not patching, config error, etc.)
  - Improper disclosure (database accessible, posting to website, etc.)
Risk Calculation

Asset, Threat, Vulnerability, Impact => Risk

(probability of event × impact = risk)
Attack Surface

Vulnerable Assets => “Attack Surface”
Contributing factors:

• Open/listening ports on outward facing servers
• Services available on the inside of the firewall
• Code that processes input
• Interfaces, SQL, web forms
• An employee with access to sensitive information is socially engineered

The Attack Surface Problem, Stephen Northcutt, SANS, 2007
Are problems in these contributing factors primarily due to mistakes (errors and omissions)?
External Attacks

Are external attacks made possible because of internal mistakes (errors and omissions)?

Caveats: offense v defense
attacker skill level

*I'm not defending the attacker nor blaming the victim*
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Date</th>
<th>Records Lost</th>
<th>Source</th>
<th>Submitted by</th>
<th>Location</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>9384</td>
<td>As many as 20,000 customers' credentials with names, contact details, usernames, encrypted passwords, and payment account information dumped on the Internet from a re-sellers' site</td>
<td>2013-03-10</td>
<td>20,000</td>
<td>Outside</td>
<td>Submitted by: lee_j</td>
<td>DE</td>
<td>Avast Germany, Procell</td>
</tr>
<tr>
<td>9318</td>
<td>Forums and user database with usernames, address (city, state, zip), country, email address, birthdate, handle/Steam ID, and possibly hashed and salted passwords accessed by intruders</td>
<td>2013-03-09</td>
<td>Unknown</td>
<td>Outside</td>
<td>Submitted by: Dissent</td>
<td>Marietta GA, US</td>
<td>CodeUSA Software</td>
</tr>
<tr>
<td>9313</td>
<td>Customers' credit/debit card numbers acquired by hackers and misused</td>
<td>2013-03-08</td>
<td>75</td>
<td>Outside</td>
<td>Submitted by: Dissent</td>
<td>Destrehan LA, US</td>
<td>Rotolo&amp;x27;s Pizzeria</td>
</tr>
<tr>
<td>9314</td>
<td>One current and one former employee indicted for obtaining the names and Social Security numbers of state inmates, filing false tax returns to obtain refunds, and cashing the checks</td>
<td>2013-03-08</td>
<td>Unknown</td>
<td>Inside Malicious</td>
<td>Submitted by: Dissent</td>
<td>Montgomery AL, US</td>
<td>Alabama Department of Corrections</td>
</tr>
<tr>
<td>9317</td>
<td>Document with employees' names and Social Security numbers exposed on intranet</td>
<td>2013-03-08</td>
<td>Unknown</td>
<td>Inside Accidental</td>
<td>Submitted by: Dissent</td>
<td>Jacksonville FL, US</td>
<td>City of Jacksonville</td>
</tr>
<tr>
<td>9310</td>
<td>Former employee inappropriately accessed approximately 1,400 patient records with names, addresses, dates of birth and in some cases, Social Security numbers and other health information</td>
<td>2013-03-08</td>
<td>1,400</td>
<td>Inside Malicious</td>
<td>Submitted by: Dissent</td>
<td>Farmington CT, US</td>
<td>University of Connecticut Health Center</td>
</tr>
<tr>
<td>9312</td>
<td>Missing flash drive contained unencrypted names, SSN, dates of birth and addresses for more than 50,000 medical providers</td>
<td>2013-03-08</td>
<td>50,405</td>
<td>Inside Accidental</td>
<td>Submitted by: Dissent</td>
<td>NC, US</td>
<td>North Carolina Department of Health and Human Services, Computer Sciences Corporation (CSC)</td>
</tr>
<tr>
<td>9238</td>
<td>Upset patient grabs other patients' information and runs out of office</td>
<td>2013-03-07</td>
<td>Unknown</td>
<td>Outside</td>
<td>Submitted by: Dissent</td>
<td>Lancaster PA, US</td>
<td>Crooked Oak Family Medicine, Lancaster General Health</td>
</tr>
<tr>
<td>9309</td>
<td>Corrections officer sold State of Florida DOC Daily Intake Lists with names, dates of birth, and Social Security numbers of inmates to confidential FBI source for use in tax refund fraud scheme</td>
<td>2013-03-07</td>
<td>805</td>
<td>Inside Malicious</td>
<td>Submitted by: Dissent</td>
<td>FL, US</td>
<td>South Florida Reception Center, Florida Department of Corrections</td>
</tr>
<tr>
<td>9307</td>
<td>Police officers misused access to Florida Dept of Highway and Safety Vehicle&amp;x27;s driver&amp;x27;s license record database (DAD) to obtain identity info which was sold to others for tax refund fraud scheme</td>
<td>2013-03-07</td>
<td>Unknown</td>
<td>Inside Accidental</td>
<td>Submitted by: Dissent</td>
<td>FL, US</td>
<td>Florida Department of Highway and Safety Vehicle</td>
</tr>
</tbody>
</table>

**HACK**

**FRAUD-SE**

**WEB**

**STOLEN DOCUMENT**
What do we do?
CERT Good Practices

- Risk assessments - insider/partners threats
- Document and enforce policies and controls.
- Security awareness training
- Secure the physical environment.
- Password and account management.
- Separation of duties and least privilege.
- SDLC - Consider insider threats
CERT Good Practices

- Consider extra controls for privileged users
- Change control
- Log, monitor, and audit
- Defense in Depth
- Secure backup and recovery
- Incident response plan

http://www.cert.org/insider_threat/
According to Schneier

Five basic techniques to deal with trusted people (Schneier):

• Limit the number of trusted people.
• Ensure that trusted people are also trustworthy.
• Limit the amount of trust each person has.
• Give people overlapping spheres of trust.
• Detect breaches of trust after the fact and issue sanctions.
Good Practices I Like

• Practical policies
• Awareness
• SDLC (SLM)
• System Review
• Vulnerability Management
• Configuration Management
• Backup
• Response/Recovery

Get the simple stuff right.
A Simple Approach

• SET briefing
  – Philosophical direction
  – Previous focus on external threats
  – New area of focus
  – Cross-divisional work – Security, IT, Privacy, Audit, Legal, Compliance
  – Culture change
Don’t let this happen to you:

April 23, 2009 Oklahoma Department of Human Services (Oklahoma City, OK):
Some personal information (names, SSNs and dates of birth for people who receive DHS services) may have been contained on a laptop computer stolen from an agency employee.

April 22, 2009 Marian Medical Center (Santa Maria, CA):
Recent patients of the emergency room and Urgent Care Center should be on alert after a Blackberry containing patient information was stolen from the hospital. The Blackberry contained an email with an attachment that had some patient information (names, SSNs, dates of birth and medical histories).

April 13, 2009 Moses Cone Hospital (Greensboro, NC):
Moses Cone Hospital is offering free credit monitoring to 14,380 patients after a laptop computer containing confidential information (including patients’ SSNs) was stolen from a VHA employee’s car.

March 7, 2009 Oklahoma Department of Human Services (Shawnee, OK):
The state Department of Human Services is investigating how a child welfare worker’s records ended up with a local TV station. The files, which included names, SSNs, contact information and details on child abuse investigations, reportedly were left behind when a DHS worker was evicted from a rental house.

March 4, 2009 Elk Grove Unified School District (Elk Grove, CA):
A document with the SSNs of Elk Grove Unified School District employees was lost by a district employee.

December 12, 2008 Oregon Health & Science University (Portland, OR):
A laptop stolen from a hotel in Chicago while an OHSU employee was there on business contained health records. The data could include medical record numbers, names, telephone numbers, dates of birth, gender, SSNs, addresses, medical diagnosis category and category of treatment — but not the specific treatments.
Examples

• Media/device encryption
• Privileged accounts/Local Admin/activity
• Improved provisioning
• Annual recertification

• Security Lifecycle Management
• Training via audio/video
• Improved server control software/logging
• Improved change/config management
To-Do List

• Communication and Awareness
• Examine current environment and resources
• Scope mitigations
• Create implementation plan
• Execute!
Where to Learn More…

- CMU CyLab - http://www.cylab.cmu.edu/
- CERT - http://www.cert.org/insider_threat/
- OSF DataLossdb - http://datalossdb.org/
- Dark Reading - http://darkreading.com/insiderthreat/
- http://slideshare.net/bcaplin
How Do You Spell CISO?

Secure360

Wed. May 14, 2014
bcaplin1@fairview.org
bc@bjb.org  @bcaplin
http://about.me/barrycaplin
http://securityandcoffee.blogspot.com

Barry Caplin
Chief Information Security Official
Fairview Health Services