Immediately Address IT Access Compliance Challenges with These Techniques, Using Tools You Already Have

Active Learning on how to Deter and Detect Patient Privacy Violations and Data Breaches by Insiders

Alan Norquist & John Vastano
Veriphyr, Inc.

Agenda: IT Compliance Deters and Detects Insider Breaches

- What is IT Access Compliance?
- Insiders more dangerous than outside hackers
  - Insiders = Employees, Contractors, 3rd Parties, Providers
- Characteristics of insider theft and privacy violations
- Why insiders bigger legal issue than hackers or lost/stolen hardware
- How IT access compliance can do what traditional IT security can’t
- Practical approaches to IT access compliance you can use immediately
Survey - Your Organization's Focus?

A. Healthcare
B. Insurance
C. Pharma
D. Medical Devices
E. Legal Services
F. Government
G. Other
H. Other/All

Survey - Your Functional Area?

A. Audit
B. Compliance
C. Compliance & Ethics
D. Ethics
E. Human Resources
F. Info Technology (IT)
G. Legal
H. Privacy
I. Risk Management
J. Other/All
IT Access Compliance

- Only have access rights as required to achieve job objectives
  - user access to systems and applications is reviewed on a periodic basis.

- Only act on data as required to achieve job objectives
  - regularly review records of information system activity

Insider = Employee, Contractor, Provider, 3rd Party or Anyone with Valid Credentials (Username and Password) including hackers with stolen credentials

You Can Keep Out the Hackers…
But Not Employees, Contractors, Providers, etc.

#1 Means of Insider Breach

Privilege Abuse

“Misusing privileges granted by a company to commit nefarious acts”

aka - Non-compliant user access

---

Selling Data Instead of Drugs?

Quotes from FBI Press Release

- “A confidential source (CS) initially approached [criminal] and inquired about purchasing narcotics.

- [Criminal] told the CS that he did not have any narcotics but that he did have personal identity information (PII) that he was willing to sell to the CS….

- [Criminal] provided the CS with specific instructions on what information to enter into the web pages of the Internet-based tax services to obtain a tax refund.

- An examination of the PII revealed that it was from a medical services provider.”
Who Commits Insider Thefts via Privileged Abuse
(Verizon 2015)

- End Users: 37.60%
- Cashier: 16.80%
- Finance: 11.20%
- Executive: 10.40%
- Other: 8%
- Manager: 6.40%
- Developer: 5.60%
- Call Center: 4%
- System Admin: 1.60%
- Help Desk: 0.80%

Data Theft via Privilege Abuse by Insiders

- Months and Years Before Discovered
  - 31.25% - stole for months
  - 18.75% - stole for years (source: Verizon)

- No Technical Skills Required
  - Already issued logins and passwords

- Walk Out of Your Organization with Stolen Data on Phone
  - No need to email or upload data to the cloud
  - Just take a photo on smart phone and walk out of the building
  - Print out or e-mail stolen data from home
Hackers vs. Privilege Abuse by Insiders – “Injury in Fact”

- Hacker Steals Patient Data
  - Did customer suffer “injury in fact”?  
  - Cases dismissed due to lack of “injury in fact”  
    - No clear connection between data theft and identity theft
- Employee Steals Data via Privilege Abuse
  - Local Law Enforcement Bust Local Identity Theft Ring
    - “Among the paperwork were computer screen-shot printouts displaying patients’ personal information from a local hospital” – indictment
  - Did patient suffer “injury in fact”? 

Stolen/Lost Computer vs Insider Theft - “Injury in Fact”

- $4 Billion Lawsuit against Healthcare Org.
  - Computer with PHI stolen
  - Dismissed due to lack of “injury in fact”  
    - “No proof unauthorized person accessed stolen material.”
- Lawsuit - Insider Theft for Identity Theft Ring
  - Police find hospital data and credit statements
  - Would this be “proof unauthorized person accessed stolen material”?
  - Would suit be dismissed?
Traditional IT Security is for Outsiders/Hackers

- Focus on the network and not designed for insider privilege abuse

IT Security Technology
- Data Loss Protection (DLP)
- Security Event Mgmt (SEM/SIEM)
- Firewalls
- Intrusion Prevention (IDS/IPS)
- Security Intelligence
- Anti-Phishing
- Anti-Virus
- Anti-Malware

Focusing on Exfiltration is Insufficient

Must detect impermissible use at the source and not depend on infiltration or exfiltration on the network or computer?

- Just Viewing is a problem
  - Geological survey results
  - M&A insider information
- Just Creating is a problem
  - Fraudulent vendors
- Just Altering is a problem
  - Company financials
Access Compliance is for Data Breach by Insiders

- Addresses privilege abuse of applications and data

Insider Privilege Abuse
+ Smartphone w/ Camera
= Data Theft

Answer: Access Compliance
- Restrict access rights to job objectives
- Monitor access activity vs. job objectives

Fraud Triangle, Privacy Breach & Access Non-Compliance

Not Being Caught for Privacy Breach Emboldens Employee Identity Theft
Fraud Triangle, Insider Breaches & Access Non-Compliance

I Will NOT Get Caught
Misusing My Access to
Sensitive Data

I’m Only Sharing
Data.
I am Not the One
Committing a Crime.

Opportunity

Pressure

Rationalization

“Unshareable”
Financial Pressure

IT Access Compliance

- Only have access rights as required to achieve job objectives
  - user access to systems and applications is reviewed on a periodic basis.

- Only act on data as required to achieve job objectives
  - regularly review records of information system activity

Insider = Employee, Contractor, Provider, 3rd Party or Anyone with Valid Credentials (Username and Password) including hackers with stolen credentials
Detect Malicious Insiders by Understanding Compliant Use

To Detect Malicious Access & Use

- Access Data or Take Actions
- OUTSIDE job objectives

Understand Compliant Access & Use

- Access ONLY the Data and Take ONLY the Action required for job objectives

Key - Use true peer groups of workers with similar job objectives
- Can’t use peer groups based on title and departments or other static label

Group workers by “job”

- If workers access or activities are anomalous for the “job”
- Then anomalous actions are impermissible use

Worker Jobs – Not Titles and Departments

All Outpatient Nurses are NOT All the Same!
Worker Jobs – Not Titles and Departments
All Outpatient Nurses are NOT All the Same!
Different Jobs Reflected in Differences in What Activities are Permissible Use

Understanding “Jobs” Reveals Impermissible Use by Nurses
IT Compliance to Proactively Detect Privacy Violations and Data Theft

- Employees Doing Similar Jobs Behave Similarly
  - Compare Employee Access Rights to Job Peers to Find Anomalies
  - Compare Employee Activity to Job Peers to Find Anomalies
    - Uses Existing Application Logs of Employee Access to Identity Data
- Investigate Anomalies with Managers and Employee
  - Employees Know They are Being Effectively Monitored
  - Deters Identity Theft (Reducing “Opportunity” in Triangle)
  - Detect Identity Theft in Early Stages
    - Intervene Before Employee Breaks the Law

Walk through examples, then hands on
Access Rights Grouped by User

- What Rights are Inappropriate?
- Insufficient context for manager to make an informed decision

Access Rights Grouped by Job Objective Peer Groups and by Application

Groups of workers who have the same job objective

Truly similar as opposed to grouping by title or department

- What Rights are Inappropriate?
### Access Rights Grouped by User

Are they all true peers? What is inappropriate?

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Worker</th>
<th>Department</th>
<th>Title</th>
<th>Scheduling</th>
<th>Pediatrics</th>
<th>Imaging</th>
<th>HR</th>
<th>FINANCE</th>
<th>EHR</th>
<th>Data Warehouse</th>
<th>BILLING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank</td>
<td>ALFA ALICE</td>
<td>Inpatient</td>
<td>RN</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ALPHA, ALPHA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BETA, BETA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRAVO, BETTY</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHARLIE, CHARLIE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DELTA, DEBBIE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DELTA, DELTA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECHO, EDWARD</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECHO, ECHO</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FOXTROT, FRANK</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FOXTROT, FOXTROT</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GAMMA, GEORGE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GOLF, GOLF</td>
<td>Inpatient</td>
<td>RN</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>KILO, KAREN</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

### Access Rights Grouped by Job Objective Peer Groups

With true peers the inappropriate access is obvious.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Worker</th>
<th>Department</th>
<th>Title</th>
<th>Scheduling</th>
<th>Pediatrics</th>
<th>Imaging</th>
<th>HR</th>
<th>FINANCE</th>
<th>EHR</th>
<th>Data Warehouse</th>
<th>BILLING</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOPG-01</td>
<td>ALFA ALICE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BRAVO, BETTY</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DELTA, DEBBIE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECHO, EDWARD</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FOXTROT, FRANK</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GAMMA, GEORGE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KILO, KAREN</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>JOPG-02</td>
<td>ALPHA, ALPHA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BETTA, BETA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CHARLIE, CHARLIE</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DELTA, DELTA</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECHO, ECHO</td>
<td>Inpatient</td>
<td>RN</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>FOXTROT, FOXTROT</td>
<td>Inpatient</td>
<td>RN</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GOLF, GOLF</td>
<td>Inpatient</td>
<td>RN</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### User Activity by Title and Department

**Is Adam Boy Acting Anomalously?**

<table>
<thead>
<tr>
<th>Worker</th>
<th>Department</th>
<th>Title</th>
<th>1/20</th>
<th>3/20</th>
<th>5/20</th>
<th>7/20</th>
<th>9/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdamBoy</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Baker</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Charlie</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Delta</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Eileen</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Frank</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Proctor</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Sam</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>George</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Idea</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>India</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Juliet</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Kiki</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Kim</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Lina</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Mary</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Mike</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Julie</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Ryan</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Oscar</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Peter</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Claire</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Sirena</td>
<td>Incident</td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

### User Activity by Job Objective Peer Groups

There are clear differences between JOPG.

<table>
<thead>
<tr>
<th>Worker</th>
<th>Department</th>
<th>Title</th>
<th>JOPG</th>
<th>Core</th>
<th>Connex</th>
<th>Common</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Omega</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Connie</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Mike</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Peter</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Claire</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Sirena</td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
<td>15</td>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Note:**
- HCCA 2017
- www.VERIPHYR.com
Live, Step-by-Step Tutorial of Techniques!

- Using Tools You Probably Already Know and Have
- Using Activity Logs and Identity Data Your Systems Already Produce
- Instructions and Examples
- Discover Identity Theft and Privacy Breach Activity
Hands-on Workshop

- Time for participants to use their own PC and Excel
- Work through real access compliance challenges
  - Identify inappropriate access rights
  - Identify patient privacy violations by insiders
  - Identify data thefts by insiders

Immediately Address IT Access Compliance Challenges with These Techniques, Using Tools You Already Have

Alan Norquist & John Vastano
anorquist@veriphyr.com
jvastano@veriphyr.com
www.VERIPHJR.com