


**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
Veriphys, Inc.



Agenda: IT Compliance Deters and Detects Insider Breaches

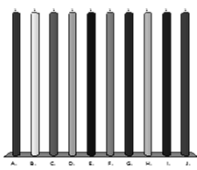
- What is IT Access Compliance?
- Insiders more dangerous than outside hackers
 - Insiders = Employees, Contractors, 3rd Parties, Providers
- Characteristics of insider theft and privacy violations
- Why insiders bigger legal issue than hackers or lost/stolen hardware
- How IT access compliance can do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

HCCA 2017 www.VERIPHYSR.com 2

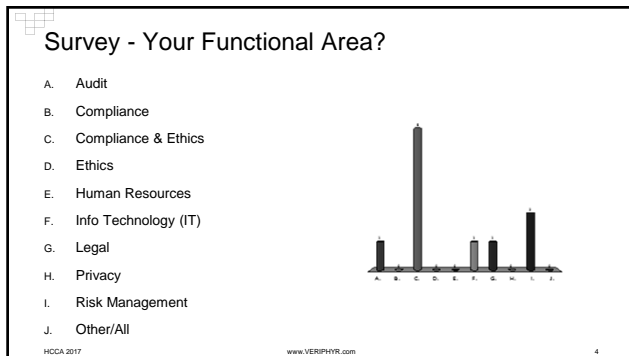


Survey - Your Organization's Focus?

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



HCCA 2017 www.VERIPHYSR.com 3

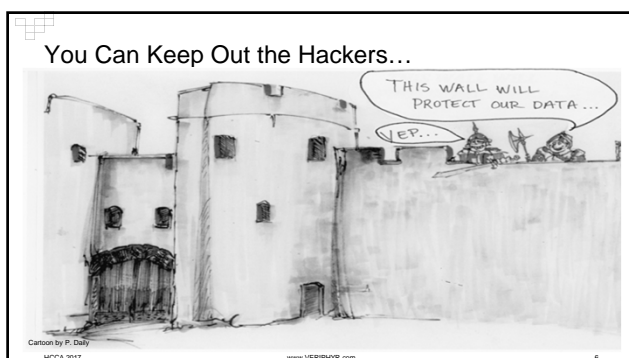


IT Access Compliance

- 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

HCCA 2017 www.VERIPHYR.com 5



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

Employee Entrance

GOOD KNIGHT, GANON

NIGHTY NIGHT, KNIGHT

Customer & Financial Data

Cartoon by P. Daly
HCCA 2017
www.VERIPHYR.com
7

Selling Data Instead of Drugs?

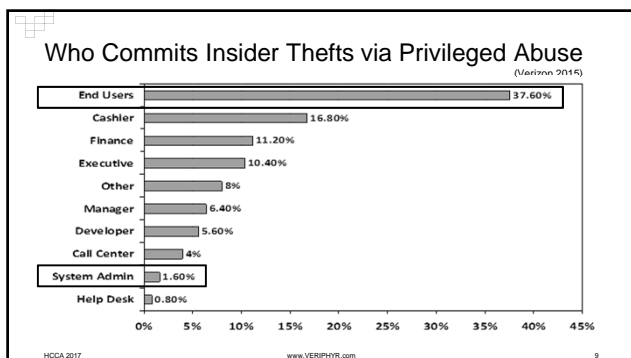
Quotes from FBI Press Release

- "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."

Drugs

PII Data

HCCA 2017
www.VERIPHYR.com
8



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



HCCA 2017

www.VERIPHYR.com

10

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”?



HCCA 2017

www.VERIPHYR.com

11

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?

Patient Hospital Screenshots



Fraudulent Credit Card Statement



HCCA 2017

www.VERIPHYR.com

12

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

HCCA 2017 www.VERIPHYR.com 13

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

HCCA 2017 www.VERIPHYR.com 14

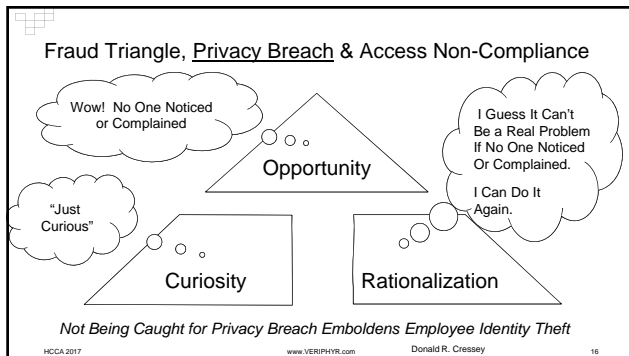
Access Compliance is for Data Breach by Insiders

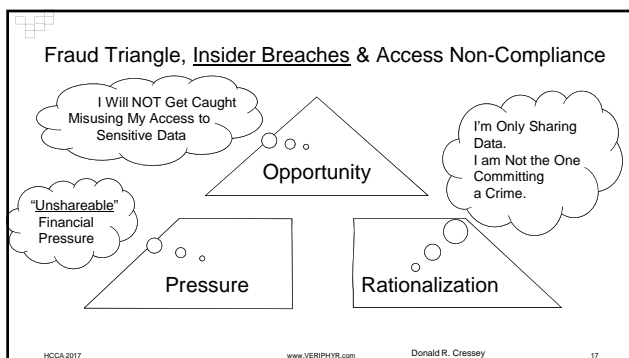
- Addresses privilege abuse of applications and data

Answer: Access Compliance

- Restrict access rights to job objectives
- Monitor access activity vs. job objectives

HCCA 2017 www.VERIPHYR.com 15





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

HCCA 2017 www.VERIPHYR.com 18

Detect Malicious Insiders by Understanding Compliant Use

To Detect **Malicious Access & Use** Understand **Compliant Access & Use**

Access Data or Take Actions **OUTSIDE job objectives** Access **ONLY** the Data and Take **ONLY** the Action **required for job objectives**

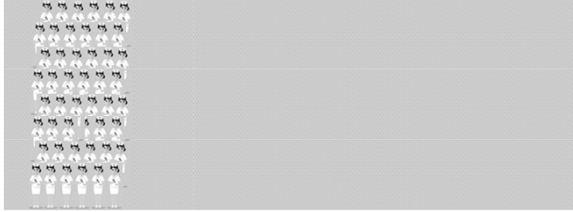
=!

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

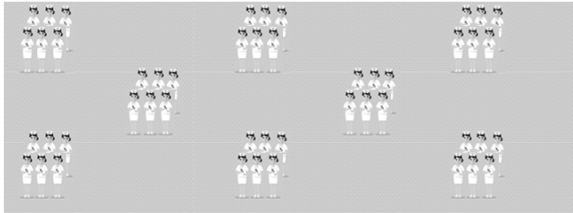
HCCA 2017 www.VERIPHYR.com 19

Worker Jobs – Not Titles and Departments
All Outpatient Nurses are **NOT** All the Same!



HCCA 2017 www.VERIPHYR.com 20

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



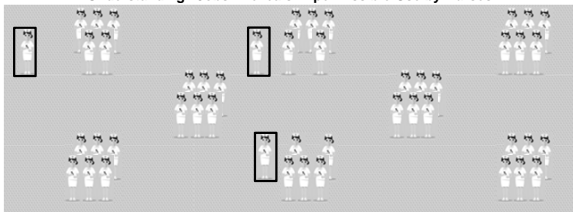
HCCA 2017 www.VERIPHYR.com 21

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



HCCA 2017 www.VERIPHYR.com 22

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

HCCA 2017 www.VERIPHYR.com 23

Walk through examples, then hands on

HCCA 2017 www.VERIPHYR.com 24

Attestation of User Access Rights

Manager: ZEBRA,ZACKARY (All User Group)

Worker	Department	Title	Application	Access Level
ALFA,ALICE	Inpatient	RN	BILLING	2
			Data Warehouse	1
			EHR	2
			FINANCE	1
			HR	4
			Imaging	1
			Pediatrics	1
			Scheduling	3
ALPHA,ALPHA	Inpatient	RN	EHR	4
			Imaging	1
			Pediatrics	4
			Scheduling	4
BETA,BETA	Inpatient	RN	EHR	4
			Imaging	1
			Pediatrics	4
			Scheduling	4
BRAVO,BETTY	Inpatient	RN	BILLING	3
			EHR	3
			FINANCE	1
			HR	5
			Imaging	1
			Pediatrics	3
			Scheduling	4
CHARLIE,CHARLIE	Inpatient	RN	EHR	4
			Imaging	1
			Pediatrics	4
			Scheduling	4

25

Access Rights Grouped by User

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

Attestation of User Access Rights

Manager: ZEBRA,ZACKARY (All User Group)

Application	Worker	Department	Title	Access Level
BILLING	ALFA,ALICE	Inpatient	RN	2
	BRAVO,BETTY	Inpatient	RN	3
	DELTA,DEBBIE	Inpatient	RN	3
	ECHO,EDWARD	Inpatient	RN	3
	FOXTROT,FRANK	Inpatient	RN	3
	GAMMA,GEORGE	Inpatient	RN	3
	KILO,KAREN	Inpatient	RN	3
Data Warehouse	ALFA,ALICE	Inpatient	RN	1
EHR	ALFA,ALICE	Inpatient	RN	2
	BRAVO,BETTY	Inpatient	RN	3
	DELTA,DEBBIE	Inpatient	RN	3
	ECHO,EDWARD	Inpatient	RN	3
	FOXTROT,FRANK	Inpatient	RN	3
	GAMMA,GEORGE	Inpatient	RN	3
	KILO,KAREN	Inpatient	RN	3
FINANCE	ALFA,ALICE	Inpatient	RN	1
	BRAVO,BETTY	Inpatient	RN	1
	DELTA,DEBBIE	Inpatient	RN	1
	ECHO,EDWARD	Inpatient	RN	1
	FOXTROT,FRANK	Inpatient	RN	1
	GAMMA,GEORGE	Inpatient	RN	1
	KILO,KAREN	Inpatient	RN	1
HR	ALFA,ALICE	Inpatient	RN	5
	BRAVO,BETTY	Inpatient	RN	5
	DELTA,DEBBIE	Inpatient	RN	5
	ECHO,EDWARD	Inpatient	RN	5

26

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?

User Access Rights Review

Manager: ZEBRA,ZACKARY (All)

Application: UOPG (All)

Access Level	Worker	Department	Title	Scheduling	Pediatrics	Imaging	HR	FINANCE	EHR	Data Warehouse	BILLING
Blank	ALFA,ALICE	Inpatient	RN	3	1	1	4	4	2	1	2
(blank)	ALPHA,ALPHA	Inpatient	RN	4	6	5					
	BETA,BETA	Inpatient	RN	4	6	5			4		
	BRAVO,BETTY	Inpatient	RN	4	2	1	5	5	3		3
	CHARLIE,CHARLIE	Inpatient	RN	4	6	5			4		
	DELTA,DEBBIE	Inpatient	RN	4	2	2	5	5	3		3
	DELTA,DELTA	Inpatient	RN	4	6	5			4		
	ECHO,EDWARD	Inpatient	RN	4	2	2	5	5	3		3
	ECHO,ECHO	Inpatient	RN	4	6	5			4		
	FOXTROT,FRANK	Inpatient	RN	4	2	2	5	5	3		3
	FOXTROT,FOXTROT	Inpatient	RN	4	6	4			3		
	GAMMA,GEORGE	Inpatient	RN	4	2	2	5	5	3		3
	GOLF,GOLF	Inpatient	RN	4	6	5			4		
	KILO,KAREN	Inpatient	RN	4	2	2	4	5	3		3

HCCA 2017 www.VERIPHYR.com 27

Access Rights Grouped by User

Are they all true peers? What is inappropriate?

Employee, Contractor, and Provider Access to Patient Data

Manager: Delta, Charlie Anomaly: Unique Key: Rare Common: Common

Activity for Single Job Objective Peer Groups
Is Adam Boy Acting Anomalously?

Worker	Department	Title	Activity 1	Activity 2	Activity 3	Activity 4	Activity 5	Activity 6	Activity 7	Activity 8	Activity 9	Activity 10	Activity 11	Activity 12	Activity 13	Activity 14	Activity 15	Activity 16	Activity 17	Activity 18	Activity 19	Activity 20	Activity 21	Activity 22	Activity 23	Activity 24	Activity 25
Adam Boy	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Charles David	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Edward Frank	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
George Henry	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Iida John	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Kirk Lincoln	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Mary Nancy	Insurgent	IN	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101	101

HCCA 2017 www.VERIPHYR.com 31

Live, Step-by-Step Tutorial of Techniques!

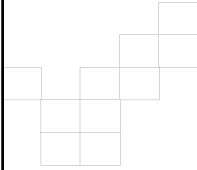
- Using Tools You Probably Already Know and Have
- Using Activity Logs and Identity Data Your Systems Already Produce
- Instructions and Examples
- Discover Identity Theft and Privacy Breach Activity

HCCA 2017 www.VERIPHYR.com 32

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

HCCA 2017 www.VERIPHYR.com 33



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

Alan Norquist & John Vastano
anorquist@veriphys.com
jvastano@veriphys.com
www.VERIPHYR.com
