Health Care Compliance Association | HCCA

Compliance Institute

Session 501: Lessons Learned: Implementing a System-Wide Access Monitoring Program

Frank DePrisco
Vice President Global Customer Operations
FairWarning, Inc.
13535 Feather Sound Drive
Suite 600
Clearwater, FL 33762
Frank@FairWarning.com
www.FairWarning.com

April 1, 2014

Today's Agenda

- Why I'm here today
- Common myths to implementing a system-wide access Monitoring Program
- Recommendations to make your monitoring effective and efficient
- Suggestions to help avoid pitfalls during implementation and on-going operations

Common Myths to Implementing an Effective Access Monitoring Program

- It will cost too much
- We don't have the time or resources (manpower)
- Our people are all trained on the laws and know not to access information without a need
- We trust our people
- What we don't know can't hurt us
- If we monitor and find inappropriate access, we will have to do something
- There will be too many false positives that will overload us

Breaking down the Myths: Myth #1

It will cost too much to monitor access

- Average cost of a data breach for an organization has dropped for the third straight time in 9 years of studies to $5.4 million, Ponemon Institute found in its 7th Annual Data Breach report.
- Total cost is not the only thing that dropped, as the average cost per compromised record decreased to $136, according to the 2013 data breach report.

Myth #1 continued

This decline suggests that organizations represented in this study have **improved** their performance in both **preparing for** and **responding** to a data breach.

As the findings reveal, more organizations are **using** data loss prevention technologies; fewer records are being lost in these breaches; and there is less customer churn.

Myth #2

We don't have the time or the resources

Based on the previous slide can we afford not to throw resources at this issue?

Often times, the issue becomes who should be responsible for the monitoring - IT or Privacy? Both play a role.

Myths #3 and #4

Our people are all trained on the laws and know not to access information without a need

We trust our people

Just look at any of the recent headlines

Understand with access to Electronic Health Records - staff develop a sense of entitlement. "Since I have access, I am entitled to look at what I want", that is unless they know you are monitoring."

Myth #5

What we don't know can't hurt us

Massachusetts General Hospital settlement with HHS: they agreed to pay $1 million and enter into a 3-year Corrective Action Plan because an employee took patient information home to work on it and left it on a commuter train.

Do you think they knew?

Myth #6

If we monitor and find inappropriate access, we will have to do something

This seems to be a common theme among organizations when it comes to monitoring. What if we find something - what do we do? I believe this is often driven because the right people are not included in the decision to monitor, what to monitor and how to process findings.

We will explore this more.

Myth #7

False Positives - It is true that a monitoring program that has not been well thought out could overburden staff due to a large number of false positives. This impact can be reduced or eliminated by taking some reasonable steps:

- Understand the workflow
- Understand what types of activity you want to monitor
- Create a good data set
- Start small, tune your alerts to eliminate false positives to the degree possible

10 Recommendations for Success

- Define clear goals
  - Compliance
  - Checking a box
  - Something greater
- Develop supporting workflows and validation process
  - Who is going to do the monitoring
  - Business or non business reason
- Develop Executive support
  - HR, Legal, Operations Officer, CMO
  - CIO, IT Managers, System Admins, DBAs

10 Recommendations for Success

- Communicate through multiple channels
  - Media
  - Education
- Ensure solution can scale
  - Number of applications to audit
  - Long term storage and expansion
- Who runs it
  - Certification training
  - Managed service

10 Recommendations for Success

- Select the right monitoring approach
  - Applications to monitor
  - Behaviors to monitor
- Assign application data experts to the project
  - Understand your data
  - Filtering of false positives
- Track incidents
  - Centralized tracking
  - Ability to report
- Have an overall governance plan
  - Measure
  - Benchmark your progress

10 Pitfalls to Avoid

- Starting to big
  - 100 systems that contain PHI
  - I want every report I can get
- Changing the scope
  - Defined for a reason
  - Weak project management
- Start a science project
  - I think there's a way you can tell me …
  - Follow the script

10 Pitfalls to Avoid

- Fail to gain full buy-in
  - Executive staff, HR
  - Line managers, staff
- Under invest in training
  - Monitoring staff
  - Organization
- Fail to include business users
  - COO, CNO
  - CMO

10 Pitfalls to Avoid

- Lack of clear documented processes
  - Tribal knowledge
  - Application upgrades
- Start backups and archives
  - Don’t lose all your hard work
- Stop maintaining your system
  - Monitoring notifications
  - Period review of user accounts, audit history, extraction code
- Not fully utilizing your system
  - Monitor your progress
  - Benchmarking

Thank you!

Health Care Compliance Association | HCCA

Compliance Institute