children's health SM

Security & Audit Tools You May Not Have Thought Of

Eric Moriak - CISSP, CISM, CGEIT, CISA, CIA
Program Manager - IT Audit

Objectives

This is not a technical presentation.

The purpose of this presentation is to share some real world examples of tools that have been developed to address the needs of a Compliance, Audit and Security function within a healthcare environment. But they can apply to other industries …

Have you -

- **… ever had to produce evidence to a regulatory body during an investigation?**
- **… locate and provide copies of management decisions or employee acknowledgements?**
- **… secure evidence that demonstrates exceptions have been properly authorized and approved?**

Outline

The following topics will be covered:

- The Scenario
- I'm an IT Auditor, why do I care?
- Some examples of tools that may help answer the tough questions
  - Policy Exceptions
  - Risk Assessments
  - Device Attestations
  - Incident Tracking
  - Application Data Mapping
- Summary

The Scenario

Here's a hypothetical scenario …

Your organization has just received a letter from the Office of Civil Rights (OCR). They want to investigate a potential breach of Protected Health Information (PHI) that occurred when an employee lost their laptop.

Let's also say that the laptop was not encrypted, it was a new beta piece of hardware and the device was running an unauthorized and unapproved application. The employee also states that they don't know how much PHI was involved and that they were unaware of their fiduciary responsibility to the organization regarding both the equipment and the data stored on the device. They further state that there has been no education informing them of their responsibilities regarding the protection of PHI.

The Scenario – Continued …

So where are you?

Does this picture help answer that question?

Better yet, what could you have done in advance to help better position the organization to prevent or defend against this review?

I'm an IT Auditor, "Why do I care?"

Internal Audit reports and work-papers can be subpoenaed. Also, as a company representative, you can be called as a witness.

Consider yourself in the following situation …

Attorney: Are you the internal auditor who last reviewed the controls over new hardware and application deployment?

You: Yes sir.

Attorney: Were your findings discussed with leadership and followed up on per IIA's International Professional Practices Framework? What did you do to ensure that the exposures as described in this case were properly actioned and resolved? What action plans were implemented and when did you perform your follow-up activities?

You: Well ….

Why Do I Care – Continued …

Technology is not always the only answer …

Besides some of the technical safeguards that <u>should</u> have been in place, are there other processes that could help mitigate this scenario?

Why Do I Care – Continued …

Let's look at the list again …

- Policy Exceptions
- Risk Assessments
- Device Attestations
- Incident Tracking
- Application Data Mapping

Policy Exceptions

Most organizations have a series of policies that address management's expectations surrounding the security and use of the enterprise's computing equipment, data, and network.

However, every organization is also going to have instances when an exception to policy needs to be granted. But when called on to prove that an exception to a policy has been properly reviewed and authorized, how do you do that?

Do you track them via email? Do you simply allow exceptions without evidence? Who owns this process, the authorizations and the documentation?

Policy Exceptions – Continued …

Email doesn't work.

Let's face it, attrition happens and if you're the third or fourth person to hold an office and an evidence of a prior exception is requested … good luck scouring your predecessor's mailboxes.

Policy Exceptions – Continued …

What you need is a process that is documented and repeatable. It should answer the following questions:

- What policy is the exception being granted for and why?
- Who is requesting the policy exception?
- Who is authorizing the policy exception?
- How long is the policy exception request going to be in effect?

It should also be:

- Easy to use
- Address your most common exception requests by default

Policy Exceptions – Continued …

Consider a requirement of a “three tier” approval process. Once the requester submits their request, it routes through three level’s of approval; their manager, IS Security, and Compliance Security. At any point in the approval chain, the request can be denied. The requestor is notified of the status at each step in the process.

Also, exceptions are automatically set to expire after one year. If not renewed by the requester or their manager, the exception will be reviewed by Compliance Security and unless acted upon, the associated exception/access will be revoked.

Having a manual review before revocation is key.

Policy Exceptions – Continued …

Common examples of exceptions can include:

- **Disable encryption**
- **Allow CD/DVD Write authority**
- **Allow USB Write authority**
- **Antivirus exclusion**
- **Obsolete OS and/or tools (possible vendor requirement)**
- **Extend session timeout**
- **Unblock web address**
- **Etc.**

Remember that supporting documentation may also be required.

Risk Assessments

Let's reconsider our original scenario …

If you recall, we had a device who's hardware and software was being "Beta" tested. In this scenario, there has also been a potential data breach.

When asked by the regulator about the controls your organization put in place over new devices … how do you respond? What configuration considerations were put in place, what additional safeguards (e.g., encryption) were implemented, what type of monitoring controls did you consider, etc.

How can you provide evidence about the decisions made in regards to the hardware/software prior to accepting the Beta versions?

Risk Assessments – Continued …

It involves another process. Risk assessments are not just another ERM exercise or an annual process in your audit function.

Risk assessments are now being required on new applications, hardware, software and even vendors. Having a process that documents the decisions made when considering one of these, will help document why your organization made the choices it made.

It can also help document who was involved and establish accountability.

Risk Assessments – Continued …

Some questions you may want to consider include:

- **Information on the item being assessed**
  - The Business Owner
  - Business Need
  - Type of data processed

- **Access Control**
  - LDAP enabled?
  - If not tied into your AD password policy, what controls are in place for length, complexity, expiration, history, etc.?
  - What types of roles exist within the application?
  - Who has the ability to modify the applications configuration?
  - Are there default or generic accounts?

Risk Assessments – Continued …

- **Hosting**
  - Internal vs. External
  - Are secured communications required? How?
  - If externally hosted, who has access to the data from a vendor perspective?
  - Is a Business Associate Agreement (BAA) in place?
  - Have SLA's been established?
  - Has a contract been signed?

- **Data**
  - Is the data encrypted in use, at rest, and/or in motion? What level (e.g. AES256)
  - If stored in a DB, has the DBMS been hardened?
  - Is data leakage a concern? If so, what controls are in place?
  - Is there logging on the application and/or DB? Is it monitored?
  - Are other tools available to access data available? If so, by who?

- **Back-ups and Contingency**
  - Is the application and the data backed up?
  - Has the restore process been tested?
  - Is this a mission critical application that requires Disaster Recovery Services?

Risk Assessments – Continued …

- **Remote Administration**
  - How does the vendor support the application … over a secured VPN?
  - Are separate accounts used for remote administration?
  - Are support accounts deactivated after each use?

- **Server configuration**
  - Physical versus Virtual
  - OS version and release control
  - Patching
  - Administrative access

- **Security Vulnerabilities**
  - Are there any known vulnerabilities (National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE))?
  - Have the servers been scanned for vulnerabilities and have risks been remediated?
  - If externally hosted, are there issues in the most recent SSAE 16 report?

Risk Assessments – Continued …

- **Policy Exceptions, are any of the following needed?**
  - Ability to write to a CD/DVD drive
  - Ability to write to an unapproved USB drive
  - Antivirus exclusion to the system or folder
  - Organization's encryption standard cannot be supported (can another be used?)
  - Blocked Websites (Do sites need to be white listed?)
  - Other

Risk Assessments – Continued …

There are also third party tools that provide industry Risk Assessment details on vendors. Do you need these as part of (or in lieu of) your assessment?

Do you have internally developed templates to ensure the consistency of assessments? Are the requirements for performing a risk assessment documented?

Who performs and manages the Risk Assessments; Internal Audit, Compliance Security, IS Security, someone else?

Risk Assessments – Continued …

Having a standardized approach (aka – template) to performing risk assessments can be key to responding to our original scenario. It can resolve issues surrounding the regulator's questions.

People will forget why they did something, even in the recent past. It's human nature. A documented approach for recording the decisions made up front on a product or a service can go a long way.

Like the scouts always say … Be Prepared

Device Attestations

Have you ever considered how many different computing devices there are in your organization?

Most IS department's have a need to track them. However, they often fall into two different populations.

The first are capital assets. These are recorded on the organization's fixed asset register for financial purposes such as depreciation. The fixed asset register is also often used for insurance purposes and tax valuations. But this is not the full list of IS devices.

The second list is often more ambiguous. These are the assets that are often expensed. However, there is often a Regulatory need for them to be tracked. For example, HIPAA requires that we track all bio-med devices, all endpoints (laptop & desktop), network gear, phones, etc. Effectively, any device that has the **potential** for storing, transmitting or processing ePHI.

Device Attestations – Continued …

So how do you do it? It's another process …

Consider requiring a device attestations on all IS issued devices.

A device attestation is an acknowledgement of an individual's accountability towards an issued device. The user must acknowledge their responsibility for the safeguarding of the asset and the data resident on that device. This acknowledgement ties back to policy.

All devices that are issued to an individual can be attested to at a single time. This includes; phones, iPad, laptops, desktops, pagers, etc.

It references policies regarding the safeguarding of assets and the sanction policy if a breach were to occur. The sanction policy includes the possibility of potential termination.

Device attestation should be required annually.

Device Attestations – Continued …

Departmental attestations are also required of departmental leaders for any devices that are assigned to their cost center … instead of an individual.

Examples

- **All equipment in the data center**
- **All MRI and CAT scanners in a radiology Dept.**
- **All bio-med devices**
- **Printers, scanners, copiers, fax machines**

Device Attestations – Continued …

Benefits include:

- **No ambiguity in regards to personal responsibility**
- **More accurate inventory records (Due to annual attestations)**
- **Increased awareness in case of loss or theft**
- **Evidence that the individual was informed of their responsibilities towards the device and its data**

Incident Tracking

Incident tracking can mean different things to different people. How many groups in your organization perform incident tracking? Here are some examples:

- **System outages**
- **Malware events**
- **Data Loss events**
- **Hotline calls**
- **Employee Complaints**
- **Escalated logging events (SIEM)**
- **Accidents**

What do each of these types of events have in common?

Incident Tracking – Continued …

A need to capture the event, document the actions taken, and to report on these events to management.

Several market based solutions exist to help manage these requirements. Effectively, they can be classified as "ticketing systems". They help monitor:

- Assignments
- Mean time to resolution
- Actions taken
- Reviews and approvals
- Linkages to other related tickets
- Manage evidence
- Etcetera

Incident Tracking – Continued …

Here are some general questions related to incident tracking …

- Who is going to do the incident investigation? What if it requires escalation to external authorities?
- What type of process do you have to conduct investigations and document the work that is performed? Is there oversight in regards to the incidents being reviewed?
- At what point are HR, Legal, and/or Executive Leadership drawn into a substantiated incident?
- Are your processes documented?
- What are your internal SLA's?

Incident Tracking – Continued …

The benefits of an incident tracking system are:

- **A documented record of individual incidents and the actions taken to resolve them**
- **The ability to perform trend analysis against similar incidents and ascertain whether patterns exist**
- **The ability to develop dashboards for executive management review**
- **The ability to classify various incidents for exposure reporting**
- **The ability to have quantifiable metrics to measure resource performance and establish metrics like … mean time to close**
- **To identify areas of both improvement or areas that require additional education**
- **Etcetera**

Data Maps

What is a data map?

In its simplest terms … it is the inventory of applications that manage a specific form of data.

In healthcare, we manage Protected Health Information (PHI). What does your business manage? Personally Identifiable Information (PII), Credit Card Information, other? What's important to you?

Data Maps – Continued …

If you have a fiduciary responsibility to manage a particular form of data … how can you do it without knowing where the data is and how it is managed?

Imagine our scenario again …

If the investigator is in front of you and asks for an inventory of all applications that process your sensitive data, what elements are processed in each application and what each application does … can you provide this to them?

Data Maps – Continued …

Again, an opportunity for another process …

A data map should show the linkage between applications and the data they manage. For example, many applications can process PHI in a healthcare environment (i.e. labs, radiology, pharmacy, EMR, etc.)

A data map describes the data and the purpose of each application as it pertains to PHI. It provides the 10,000 foot view of the environment with the ability to understand the interfaces between applications.

Data Maps – Continued …

At a healthcare provider, IS' primary data responsibility is in regards to PHI. The data map provides the inventory of applications and the data they process.

Without it, how could a healthcare organization state that they are in compliance with HIPAA if they don't even understand what systems process health information?

If you have similar compliance requirements for SOX, PCI, GLBA, FFIEC, etc., do you have a list of all systems.

Data Maps – Continued …

For many organizations, the PMO (Project Management Office) owns the data map.

It is a template based approach. Every time an application is added or updated within our environment, the template must be completed or refreshed. These forms are then managed by the PMO and inquires can then be made against that data.

By managing the inventory of applications at the source … you can have confidence that your data map is current and comprehensive for those elements you are interested in.

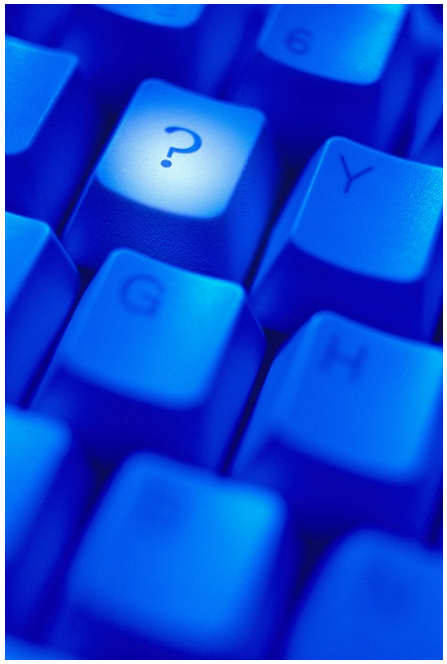
Summary

IT Audit is not simply checking security configurations and performing vulnerability assessments.

A value added IT Audit and/or Security function helps prepare an organization for situations that are on the horizon and helps to defend an organization during regulatory scrutiny.

Internal Audit is uniquely positioned to help advocate procedural improvements that an organization can leverage to improve its awareness and overall control environment.

Simply Put: *Do not go up the creek without your paddle …*



Questions?