SailPoint

WHITE PAPER

Managing Healthcare **Insider Security Threats**

Healthcare provider organizations are fighting back against those who attempt to access sensitive data for questionable motives. As a one-stop shop, provider organizations possess Protected Health Information (PHI), Personally Identifiable Information (PII) and even Payment Card Industry (PCI) data – all of which are sought after on the cyber-crime black market. In some cases, where medical research is conducted, the provider organization must further concern itself with governing access to research data.

While most providers are leveraging various technology to keep outsiders out of their IT infrastructure, the information security gap continues to widen because data exposure is often due to someone from within the organization.

While much of the media has focused on external breaches and would-be hackers, the overwhelming majority of healthcare provider respondents see insiders as an equal or greater threat to unwanted exposure of sensitive data.

I. Methodology

HIMSS Media conducted a study on behalf of SailPoint in April 2018 to better understand how hospitals and health systems perceive and manage insider threats to cybersecurity. A total of 101 qualified respondents completed the survey.

Figure A

- Respondents were screened for involvement with cybersecurity purchases/initiatives.

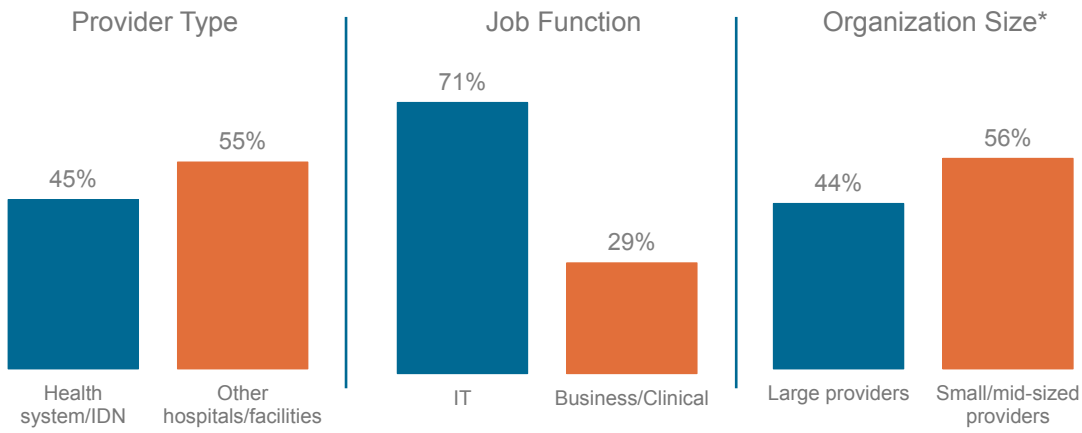
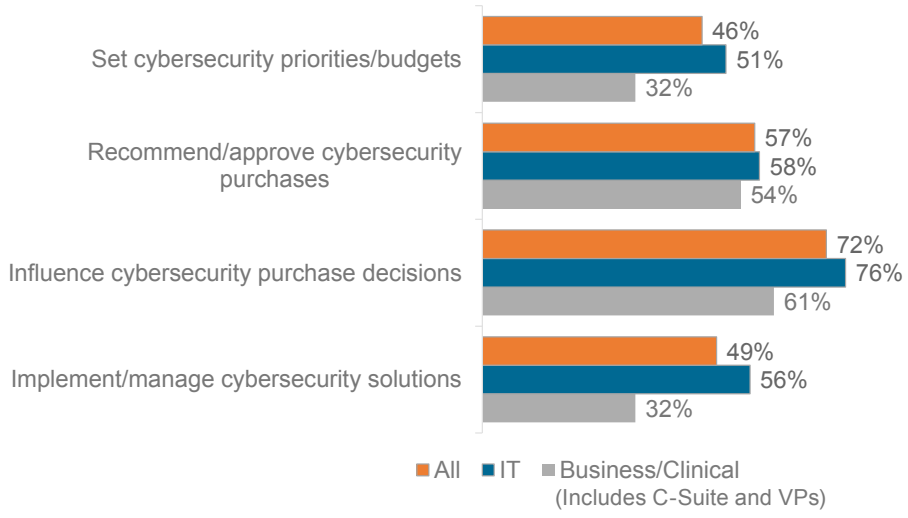


Figure B



II. Understand the Insider

Insiders cannot be defined simply by their employed status. Today, provider organizations must look at insiders through the lens of application and data access entitlements. This would typically include employed- and non-employed staff, volunteers, vendor partners, contractors and even patients who access their personal health records via online portals. Each of these individuals may expose sensitive data for any one of three reasons.

- **Accidental** – Unauthorized exposure of sensitive information is often the result of users lacking awareness of processes or best practices.
- **Negligence** – Users who knowingly disregard established policies due to negligence have various reasons, but their intent is not malicious.
- **Malicious** – Users who are malicious intentionally expose sensitive data for various reasons, whether for financial gain, espionage or something else.

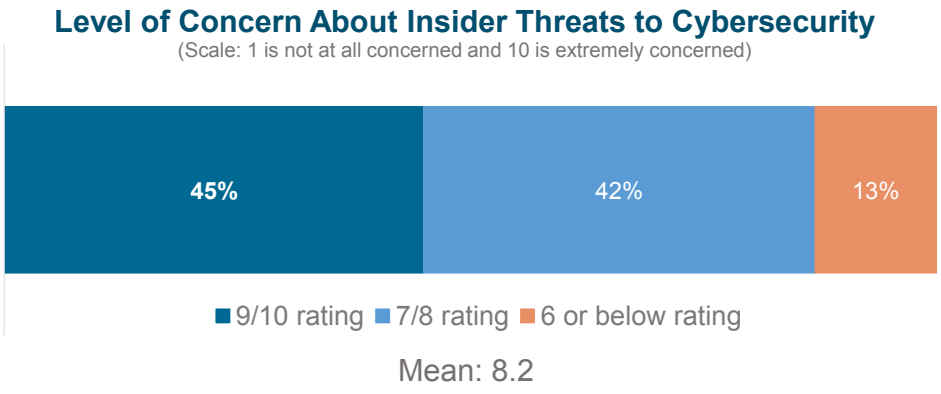
III. Study Findings

1. Healthcare provider organizations share widespread concerns regarding risk of insider threats to cybersecurity.

With a mean score of 8.2 out of 10, the responses from healthcare organizations indicate an acute level of concern around the threats posed by insiders (Figure 1).

Given that provider organizations now govern thousands of digital identities, both human and devices, with thousands more unique access requirements, this level of concern is justified and could likely growl.

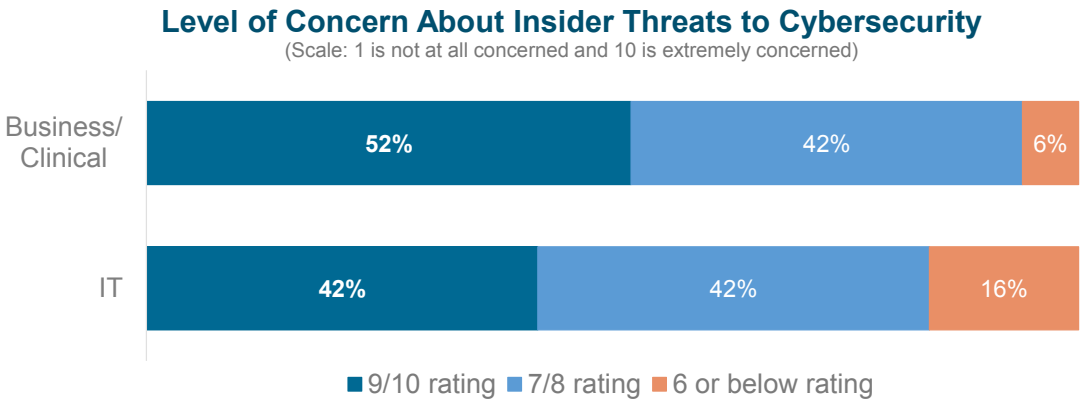
Figure 1



Digging deeper, the study indicates a noticeable difference between business and clinical respondents versus those who work in IT. In Figure 2, 52 percent of non-IT respondents rate their concerns around insider threats, at 9 or 10. This is a 10-point difference compared to IT respondents. Typically, business and clinical leaders

are not as close as IT professionals are to the actual process of governing access. However, should an event occur, the remediation process will likely have a negative impact on operational workflows – a fact that seems to be understood by these end users.

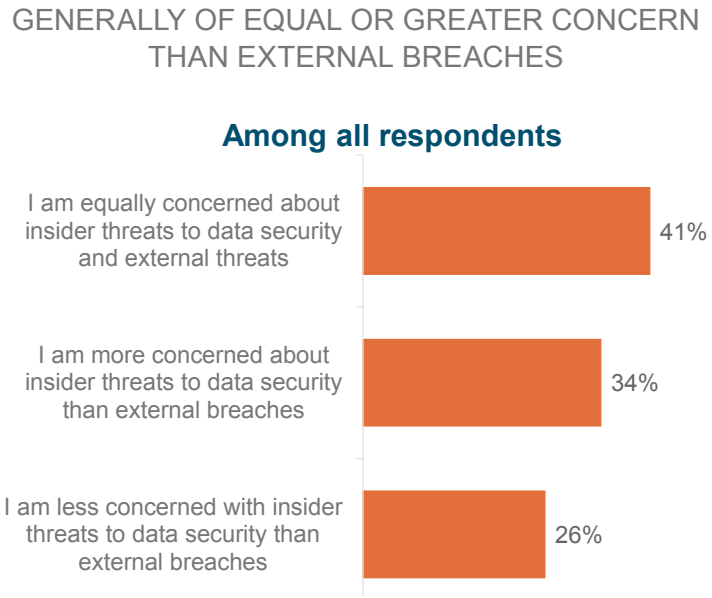
Figure 2



2. Insider threats are generally of equal or greater concern to hospitals and health systems than external breaches.

In Figure 3, we learn that while much of the media has focused on external breaches and would-be hackers, the overwhelming majority of healthcare provider respondents see insiders as an equal or greater threat to unwanted exposure of sensitive data. In fact, among those implementing or managing cybersecurity solutions, 43 percent stated insider threats to be of greater concern than outsider threats.

Figure 3

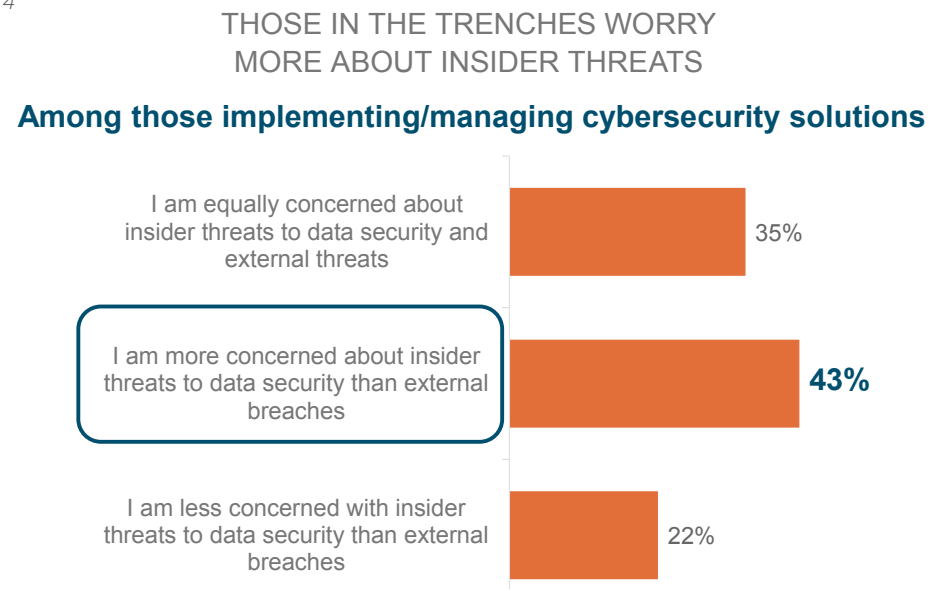


Interestingly, during the HIMSS national conference in March 2018, many of the information security presentations were focused on keeping outsiders out of the IT infrastructure. The looming topics that were seldom addressed include:

- What do you do once someone with malintent gets inside?
- What if the threat originated from an insider?
- How would you mitigate insider risks beyond awareness and training?

These issues are also on the minds of many healthcare providers.

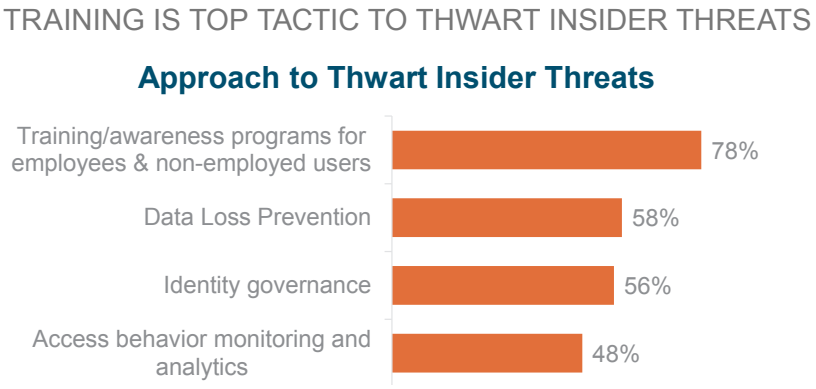
Figure 4



3. While training and awareness are currently the most used tactics for thwarting insider threats, too many are leaving gaps by not deploying critical technology that enable secure governance.

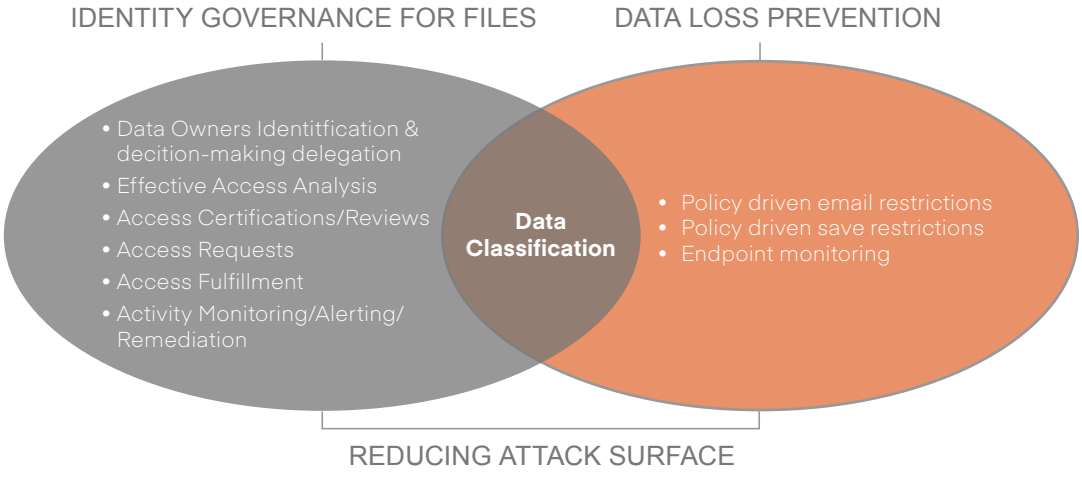
Training continues to be a staple for addressing threats posed by insiders. In Figure 5, 3/4 of the respondents rely on this tactic. However, training without enablement tools and technology is insufficient for closing critical security and even compliance gaps. As indicated in the study, roughly half of the respondents are leveraging Identity governance for data stored in files or data loss prevention (DLP) tools.

Figure 5



In general, DLP technology allows healthcare providers to intervene with improper handling of data in motion through data classification with rules. Identity governance can intercede before the file is captured by DLP and mitigate risk of access to sensitive files by users who should not have that entitlement to begin with. When applied together, these solutions complement one another to provide prevention and intervention capabilities (Figure 6).

Figure 6



4. A unified governance approach to digital identities and their access continues to mature, but has room to grow.

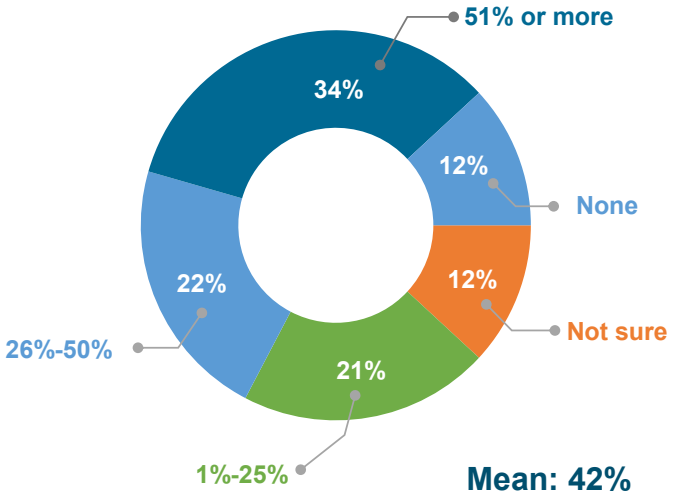
Disparate processes around identity governance is an Achilles heel for healthcare providers. Governing digital identities and their entitlements to systems and applications require a consistent and unified approach. This allows organizations to reduce delayed access for users, avoid improper or inconsistent provisioning, and reduce workload for IT administrators and data stewards. Ultimately, a unified identity governance approach translates to stronger security and compliance, better operational workflow for users and greater cost efficiencies.

Unfortunately, too many provider organizations have not incorporated most of their applications, or even files, into a unified governance approach. This suggests many healthcare organizations are operating with large gaps in their security and compliance efforts. Given that provider organizations are continuously on-boarding and operating numerous applications, it is imperative that these critical gaps are addressed to protect sensitive information stored in systems, applications, and file storage folders. Doing so allows providers to:

- Align policy and centralizing access controls across the organization
- Automatically grant and revoke access based on training criteria
- Eliminate stale entitlements through automatic certification campaigns
- Give managers visibility into what access their direct reports have
- Detect, document and alert appropriate security teams regarding any attempts to circumvent governance processes

Figure 7

2/3RDS HAVE INCORPORATED LESS THAN 1/2 OF THEIR APPLICATIONS INTO AN IDENTITY GOVERNANCE PROGRAM



5. In general, there remains a deep reliance on antiquated processes to govern data stored in files.

The collaboration and sharing of information needed by modern healthcare organizations to deliver excellent patient care can create blind spots where sensitive data is not well-protected. One of the most significant examples of this occurs during the data lifecycle.

As patient data and other sensitive information are extracted from applications and databases, it is often manipulated and saved in file formats such as PDFs, presentations, text documents and spreadsheets. These files may be edited further, resulting in multiple versions being stored in a variety of locations, and some of these locations may not be secure. Here are just a few examples of how this happens:

Copied and Pasted Information

- A clinician conducting a research study may copy and paste medication administration or flowsheet data from the Electronic Health Records (EHR) system into an application such as Word, PowerPoint or Excel for tracking.
- An assistant may copy and paste historical data for the day's scheduled visits into Word for a provider's consumption outside of the EHR.

Reports

- The provider organization's Health Information Management department may run a real-time operational report for auditing purposes. The report may be later saved to a network drive for future reference.
- Overnight EHR batch reports may be run and distributed on a network drive or SharePoint site.

Scanned Documents

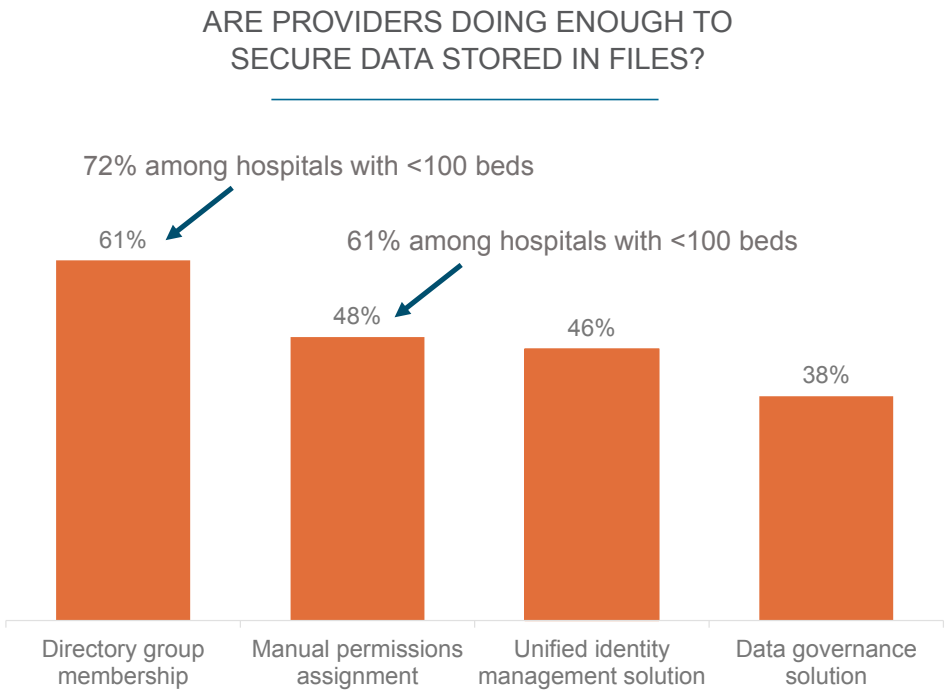
- Insurance cards and other enrollment paperwork may be scanned when the patient is admitted. Later, it may be downloaded by Patient Financial Services to work on the file.
- Occupational Health records not stored in an EHR may be scanned and stored in folders on a network drive.

To secure these data files, we learn In Figure 8 that 61 percent leverage directory group membership. While theoretically possible, applying the principle is much more difficult due to inherent challenges with group membership nesting. In practice, it is nearly impossible to properly control access without the proper tools. Much like an individual committing a New Year's resolution to run five miles a day, training, processes and tools are necessary to make this possible.

The same chart indicates 48 percent use manual permissions assignments to govern the vast and ever-growing volume of data stored in files. This is extremely inefficient, difficult to manage and simply cannot be effectively scaled. Thus, security gaps often exist where manual permissions assignments are used.

It seems many healthcare providers are deficient in securing their data and are not deploying a holistic identity program that includes these files.

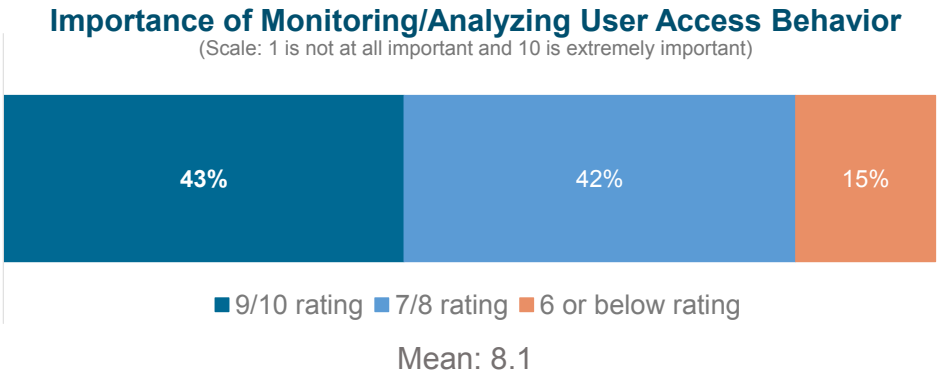
Figure 8



6. Importance of monitoring/analyzing user access behavior is widely accepted, yet most have not fully achieved this capability.
As seen in Figure 8, most provider organizations have yet to move beyond directory group memberships. However, in Figure 9, respondents view the ability to monitor and analyze user access behavior of utmost importance. To achieve this, tools with sophisticated capabilities are required. Moreover, as the healthcare space continues to evolve and become increasingly complex, the aid of identity analytics-based artificial intelligence and machine learning will likely become a critical part in gathering and synthesizing access data to provide deep contextual insight and recommendations.

Figure 9

ABILITY TO MONITOR/ANALYZE USER ACCESS BEHAVIOR OF HIGH IMPORTANCE



IV. Conclusions

The insider threat to information security within healthcare provider organizations has become a top concern. In fact, many respondents consider insider threats an equal if not a greater risk than an unauthorized intrusion from the outside. Unfortunately for most organizations, the concerns are not being adequately met.

While training and awareness programs remain a commonly deployed tactic, organizations are falling short of providing the proper tools and technology that enable best practices. Healthcare providers seeking to mitigate insider risks would be wise to consider adopting a truly comprehensive, intelligent identity solution as a foundation for governing and protecting on-premises or cloud applications and data files.

WP1234-1807