Insider threat in life sciences

2018 Program benchmark report

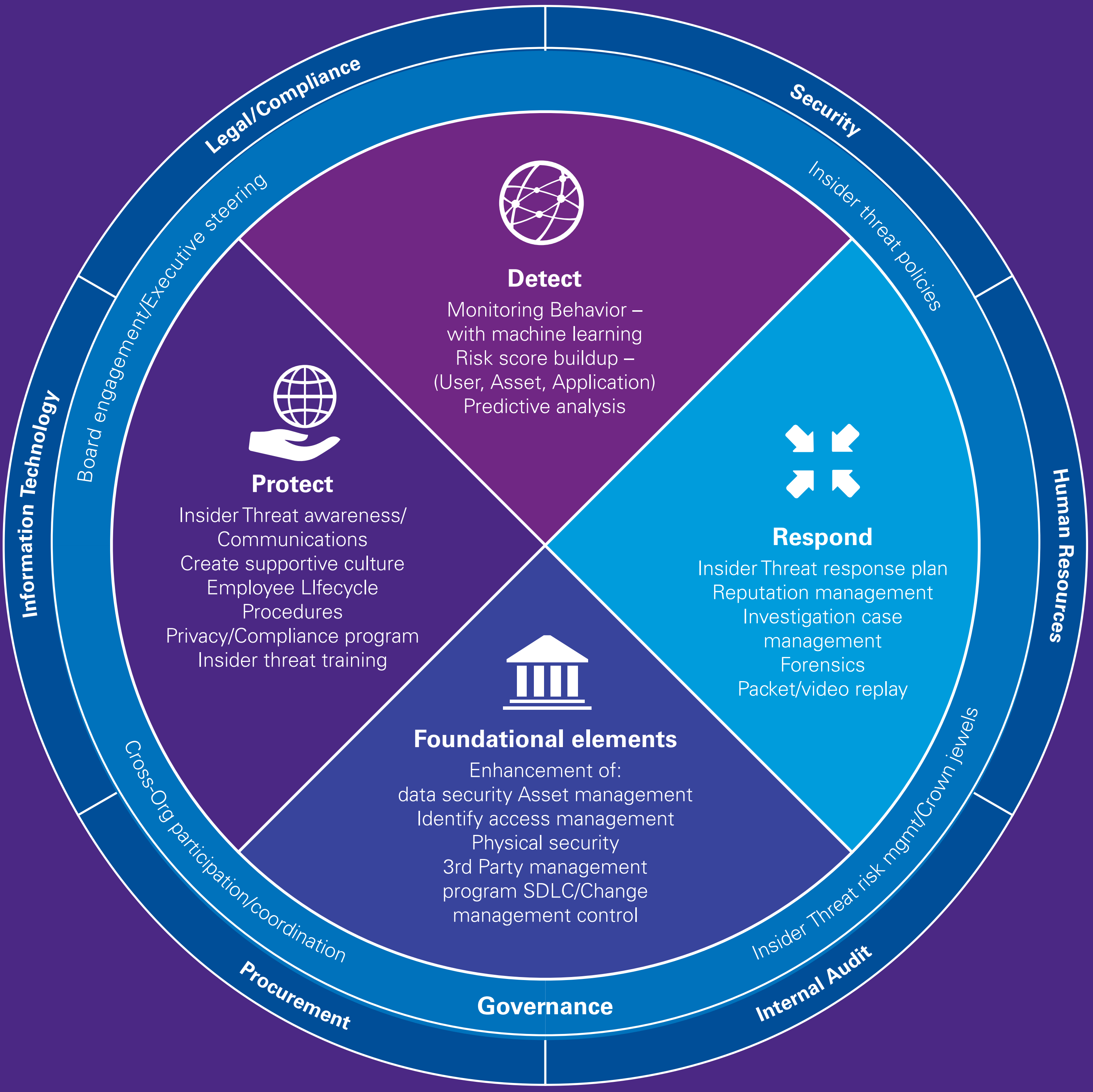
May 2018

kpmg.com

The mission critical information, assets and operations of life sciences organizations are coming under attack – from within. The historic perspective of addressing external threats is no longer enough. But dealing with threats from the inside, both intentional and unintentional actions from employees, contractors and third-parties, involves many new challenges such as privacy issues, cultural impacts, behavioral patterns and ways of working. Just knowing where to start is a challenge.

This report collected information from participants in Pharmaceuticals, Crop Science and Consumer Health areas. Respondents average over $30 billion annual revenue and over 65,000 employees. Our approach entailed interviewing senior executives about where they are in developing their Insider Threat programs. From this input, we have derived observations, trends and insights on leading practices in the area.

KPMG has defined a framework of the elements of an Insider Threat program. These elements include Program Governance, Protect, Detect, Respond and "Foundational" elements (those that are outside of an Insider Threat Program proper but are important in providing a base to support the program's needs). The results of this benchmark study will follow these framework areas.



Legal/Compliance

Security

Human Resources

Internal Audit

Governance

Procurement

Information Technology

Board engagement/Executive steering

Insider threat policies

Insider Threat risk mgmt/Crown jewels

Cross-Org participation/coordination

Detect

Monitoring Behavior –
with machine learning
Risk score buildup –
(User, Asset, Application)
Predictive analysis

Protect

Insider Threat awareness/
Communications
Create supportive culture
Employee LIfecycle
Procedures
Privacy/Compliance program
Insider threat training

Respond

Insider Threat response plan
Reputation management
Investigation case
management
Forensics
Packet/video replay

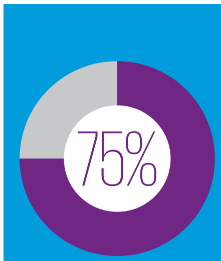
Foundational elements

Enhancement of:
data security Asset management
Identify access management
Physical security
3rd Party management
program SDLC/Change
management control

Table of contents

Overall program/ governance findings

We begin by looking at Insider Threat at the program level. It is helpful to understand where programs are in their development, how they are structured, etc. Overall, we found that Insider Threat is an important topic with the majority of respondents, 75%, having active Insider Threat programs. Yet, this is still in its early stages with about two-thirds of programs being cited as “in progress”. It was noted that most programs are building on current investigation efforts, expanding them into more comprehensive Insider Threat operations. Many of these efforts are starting with manual processes with a periodic meeting cadence but are looking to move to a more automated approach.

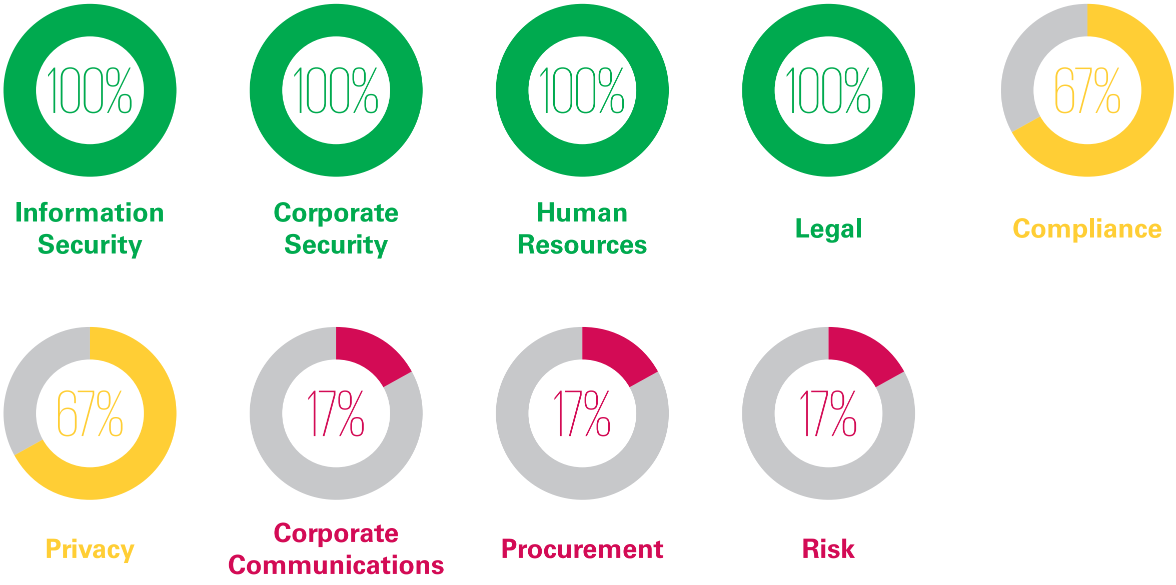


having active **Insider Threat programs**

Yet, this is still in its early stages with about **two-thirds of programs** being cited as “in progress”

It was noted that most programs are coming out of expansions of current **investigation efforts**

A critical and challenging aspect of building and Insider Threat program is bringing together the various relevant areas in an organization to work together in a unified approach. Accordingly, one of our questions focused on which of those areas were most commonly included in the program. KPMG and CERT/Carnegie-Mellon recommend including the following areas in a program as shown. We found that only a small minority included all areas. The proportion of each is shown below:



Building an empowered team

The first step is to link together all of the constituents in your organization who play a role in addressing Insider Threats: information security, physical security, investigations, legal and compliance, ethics, worker/labor relations, contract labor management, Human Resources and risk management, just to name a few. An Insider Threat program manager should be named and empowered by leadership to work across these areas in a unified manner.

Other general findings regarding overall Insider Threat programs are as follows:

Spend is increasing – Though spend in this area has historically been somewhat low, this is changing. Of those changing spend toward Insider Threat programs, increase outweighs decrease by 4:1.

Most do NOT call it an "Insider Threat" program – The naming of a program (provided it is not secret) is a crucial decision as it sets the tone with the general employee populace. Almost unanimously, programs are not going by the name "Insider Threat" or Insider Risk" with most opting for names such as "Critical Asset Protection", etc. Most were still wrestling with this difficult decision and reported that they did not yet have a name for the program.

Half of programs are accountable to the CISO where the other half reported a range of reporting relationships with no trend among respondents. Others included reporting to the CEO, the CFO or even stand-alone without a strict reporting relationship. It is interesting to note that no programs reported through the Office of General Counsel which is one of the primary models recommended by the CERT group.

Most are at least somewhat secretive – Approximately 60% of respondents noted that their programs were either secret/concealed from the general employee/third-party base or had significant portions of their operations that were not shared.

Beginning at the beginning – Crown Jewels analysis

Before embarking on the creation of an Insider Threat program, an organization should undergo a formal definition of its business drivers and "crown jewels." This includes assets and information as well as business functions that are at risk: clinical trials, R&D, production capacity and others. Finally, it is important to remember that Insider Threat motivations may often lead to events that involve things other than data, including workplace violence or product sabotage.

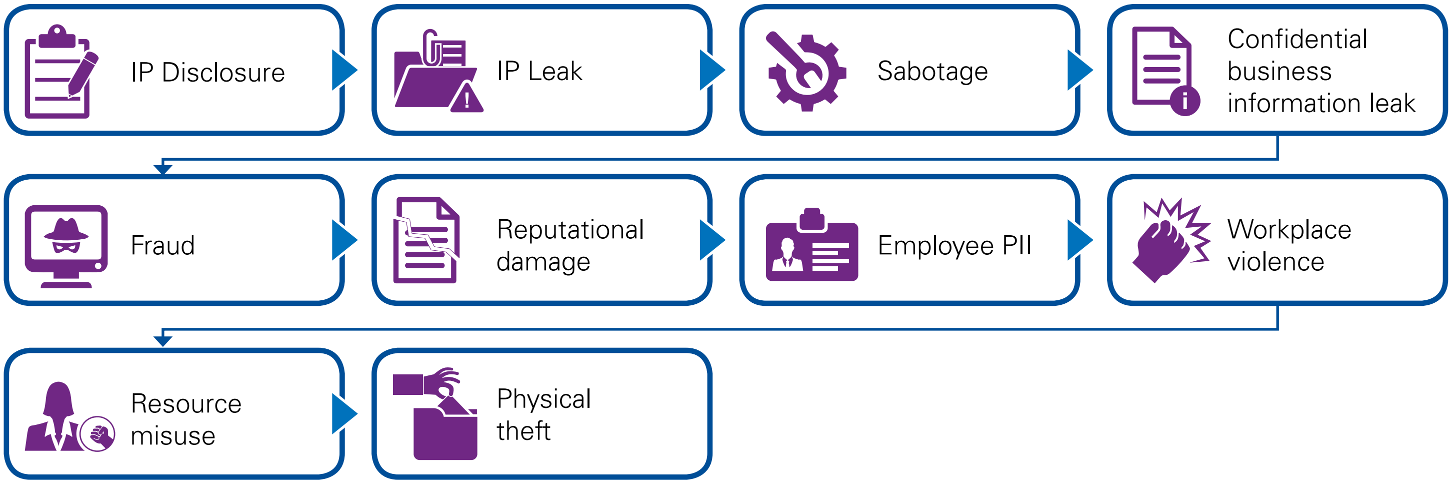
Our study found that all respondents viewed this exercise as important but were at different points in the process currently. About half of the respondents have conducted such an exercise with the other half in process or planning (33% and 17% respectively). Not surprisingly, the more mature programs tended to have a better grasp of their crown jewels picture. As an additional note, the majority of respondents consider more than just information in their crown jewels definition whereas only about one-third limited it to information.

Beginning at the beginning – Threat profiles

Another crucial early step is gaining an understanding of the actors and motives that drive the threat by conducting a threat profile analysis. This analysis gives a basis for which risk scenarios the program seeks to manage: workplace violence? Inadvertent or intentional data leakage? Business process sabotage? Once the scenarios are mapped, specific processes and technologies can be implemented (or often, repurposed from existing implementations) to protect, detect and respond to different insider scenarios.

Our findings in the area of threats showed that intellectual property loss/leakage is foremost on the minds of most respondents - This is not surprising for the Life Sciences vertical.
The concern areas in descending order of importance are as follows:

— Concern areas, in order



IP Disclosure

IP Leak

Sabotage

Confidential business information leak

Fraud

Reputational damage

Employee PII

Workplace violence

Resource misuse

Physical theft

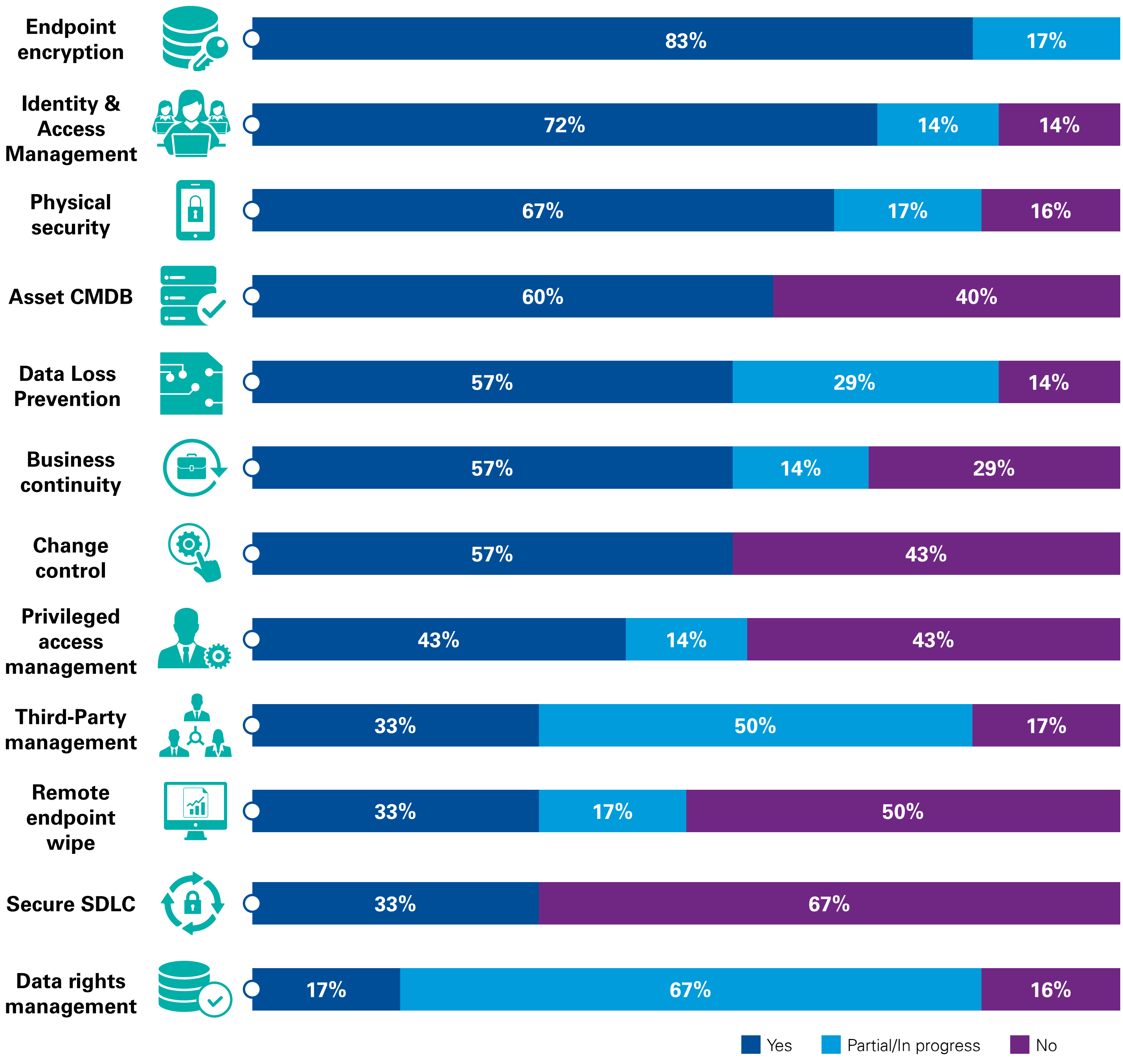
The most worrisome threat actors seem to be malicious employees, followed by malicious third-parties. The intent seems to be of more importance than the category of actor since the third and fourth most important actors are the unintentional (employee and third-party respectively).

> **It's interesting to note that, though malicious intent is the most concerning to the surveyed organizations, up to two-thirds of insider incidents are actually due to unintentional actor activity.**
>
> — ***Michael Thompson,*** *Director, KPMG*

Foundational area findings

There are several programs that are usually outside of an Insider Threat Program but are important in providing a base to support the program's needs. These are referred to as "Foundational" elements. These represent opportunities to leverage your investment in these existing programs to support and strengthen an Insider Threat program. We explored which of these foundation elements are typically playing a part in programs in the Life Sciences area. We found the following among our respondents:

Foundational elements:

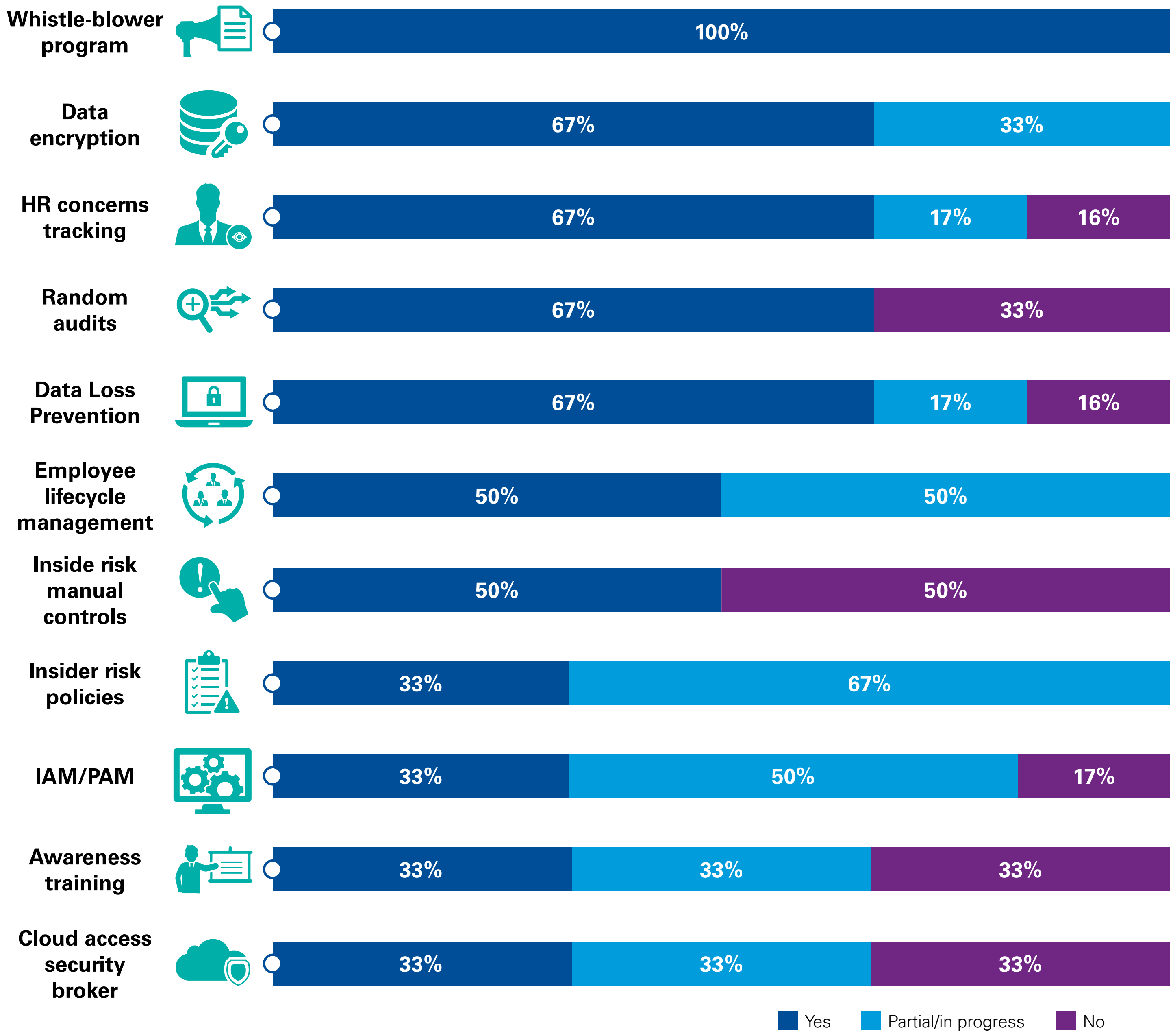


The foundation of information classification and access
The failure to understand foundational elements such as what constitutes sensitive data and how to control access to that data to a least-privileged basis can lead to a larger attack surface to Insiders.

Protection-related findings

Unlike many areas of security, the "Protect" portion of the Insider Threat area is less about tools and more about programmatic measures that consider the cultural aspect – Keeping a happy, engaged base of employees can be the best first step in preventing Insider Threats. One of the main goals of Insider Threat prevention is to reduce the tendency for employees to become threats in the first place through improved employee engagement, programs that increase satisfaction and that allow employees to feel they have a voice, etc. Examples of these protection measures and their prevalence across our Life Sciences benchmark group is as follows:

Protect programs:



Frequently, organizations fail to arm their employees, contractors and suppliers with the technology and awareness needed to adhere to processes and rules while still effectively operating the business. Doing so forces even high-performing and conscientious parties to engage in risky “get it done” behaviors outside of approved channels.

— ***Gavin Mead,*** *Principal*
Cyber Defense Lead, KPMG

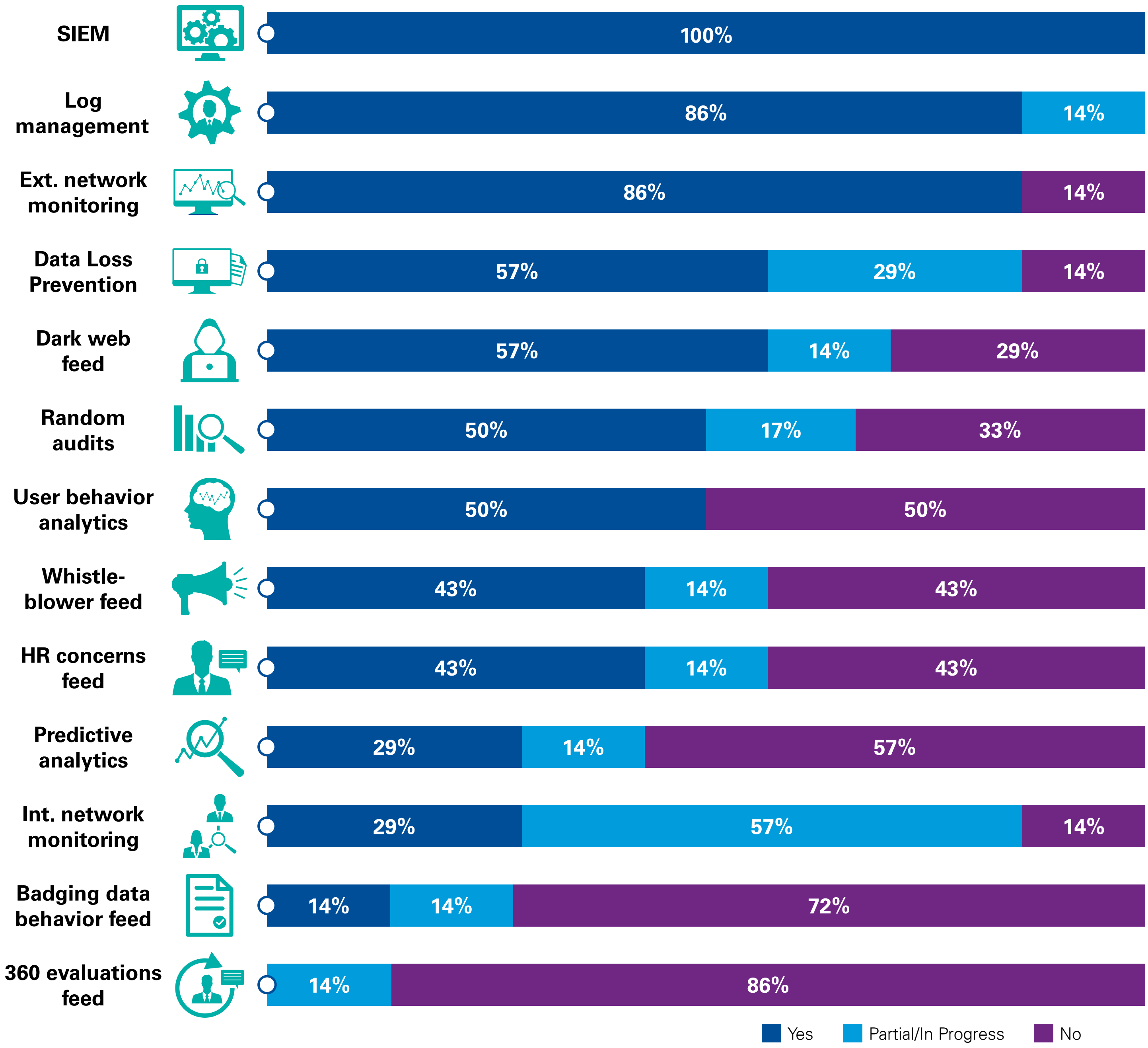
Cultural aspects of protection

Employees must understand that the program is designed to protect everyone’s job and livelihood and not perceive it as “big brother “driven by employer mistrust. Programs that fail to create this positive perception with employees can actually be the cause of disgruntlement, becoming part of the problem they are attempting to solve.

Detection-related findings

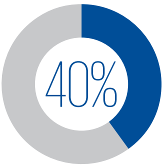
Detection of Insider Threats is a far greater challenge than detecting threats from the outside. After all, the Insider Threat is, by definition, someone you've "given the keys to" via network credentials, physical access, etc. Traditional techniques such as looking for malware signatures, suspicious IPs, etc. are not sufficient. Instead, behavioral patterns and anomalies from peers and histories must be discerned and risk scores built from many "small, faint signals" in daily activity. There are many detection tools, both technical and non-technical. Our study found which were most common across the benchmark respondents:

Detection tools and techniques:

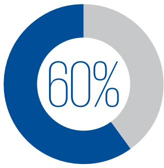


It is interesting to note that although half respondents are pursuing UEBA (User/Entity Behavior Analytics), very few are feeding it with log sources different from their standard SIEMs (Security Information and Event Monitoring) systems. This implies that the ability of most to detect insider activities will likely be hampered.

— Percentage of population monitored: When asked what proportion of their employee/third-party base was being monitored, we found that the answer varied widely with:



targeting all of their users and



targeting only a small percentage of their base.

For those only monitoring a subset, they cited that it was due to starting the program with a small, manageable user set or driven by specific cases.

— Monitoring of Third-Parties – As a final observation around detection, we found that about half of respondents took steps to actively monitor their third-party partners. This acknowledges the dependence they have on their partners and if there are weaknesses in that partner's security, that puts them both at risk.

Detecting Insider Threat

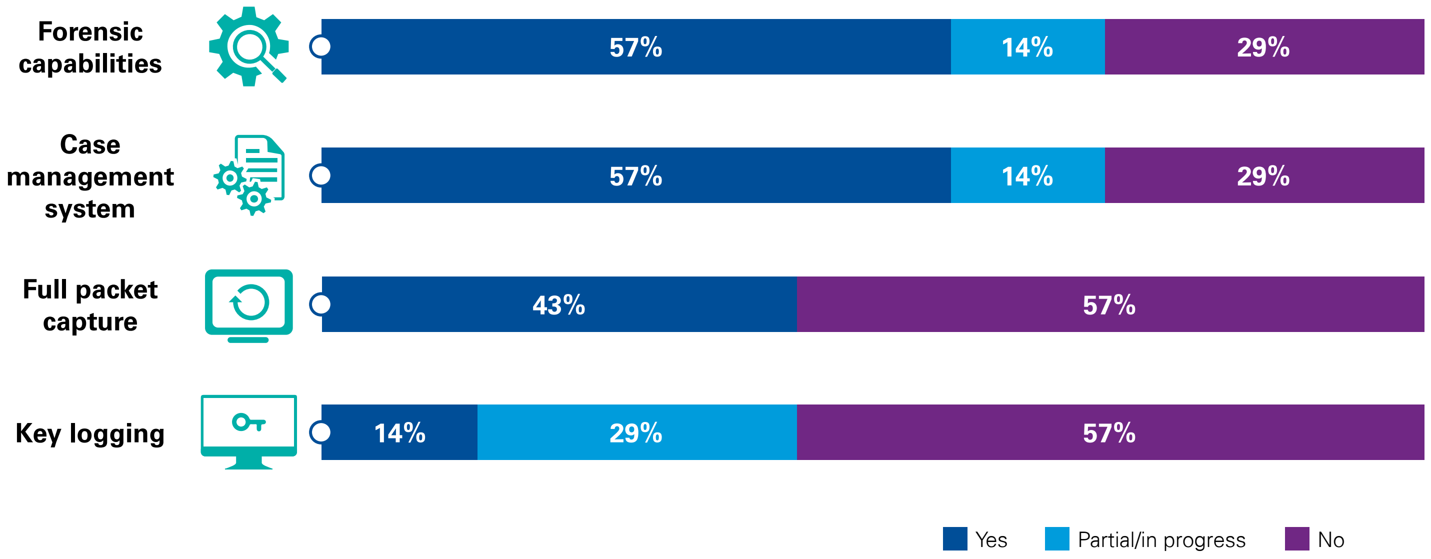
Most organizations think of user behavior analytics as the primary means of monitoring for Insider Threat. Though this relatively new area is often not yet mastered by many programs, it is a key element and holds a lot of promise. But, Insider Threat requires a high degree of non-technical monitoring as well: whistle blower programs, HR issues, periodic background/credit checks, etc. All of these must be considered and coordinated together to create a true picture of insider risk.

Response-related findings

Responding to Insider Threat incidents is especially complex and challenging. In addition to requiring a cross-team coordination and proper empowerment, the program must also consider the privacy rights of its employees, the legal and cultural implications of the investigating its employees. More than any other areas covered thus far, the Response area also has a high-degree of coordination with outside parties such as law enforcement, forensic specialists, etc.

The tools for handling Insider Threat Response range from simply tracking the steps of an incident's investigative process to detailed technical analysis and "playback" of the activity of an insider's activities. Not surprisingly, the "basics" such as case management and forensics are common while fewer have the detailed playback capabilities of full-packet capture and key logging:

Response tools:



Our reporting found that all respondents with active Insider Threat programs have cross-functional participation in their investigation process. Additionally, all participants have documented major incident response plans.

Automating the Hub with case management

Programs often start with a manual process of periodic "Hub" meetings. These bring together representatives from all participating areas across the organization to compare notes on concerns they have with potential and active Insider Cases. A good next step to improve this somewhat arduous and slow process is to move these areas to a common case management platform. This allows faster and more efficient visibility and workflow management as the program begins to breakdown silos and work as a cross-functional effort.

When looking across the three operational areas of Protect, Detect and Respond, we found that the spend across the three was fairly even (as shown below). The Respond area was a bit higher. This could be due to where most programs are in their maturity curve which places them in a re-active mode, placing emphasis on dealing with issues. It could also be partly due to expensive third-party forensic service requirements.

- Spend focus:
  - Protect: 30 percent
  - Detect: 29 percent
  - Respond: 36 percent

The average staffing for the three areas were found to be as follows:

- FTEs:
  - Protect: 4
  - Detect: 8
  - Respond: 4

Handling Insider Threats is still a relatively new challenge for many Life Sciences organizations. It is growing increasingly important as threat trends continue and companies become more aware of what is at risk. We hope you have found this report informative and helpful for understanding how Life Sciences organizations are addressing this growing challenge as you consider your own needs in this area.

Contact us

Sarat Mynampati
Managing Director
Life Sciences Lead
T: 973-912-6126
E: smynampati@kpmg.com

Michael Thompson
Director
Insider Threat Lead
T: 832-689-4475
E: mdthompson@kpmg.com

Gavin Mead
Principal
Cyber Defense Lead
T: 404-353-3179
E: gmead@kpmg.com

kpmg.com/socialmedia