Insider Threats and the Need for **Fast** and **Directed Response**

Lorem ipsum

Veriato

www.veriato.com

Many organizations design their networks in a way that enables accidental as well as malicious insiders to cause significant damage.

As breaches continue to cause significant damage to organizations, security consciousness is shifting from traditional perimeter defense to a holistic understanding of what is causing the damage and where organizations are exposed. Although many attacks are from an external source, attacks from within often cause the most damage. This report looks at how and why insider attacks occur and their implications.

Why focus on insiders? Because they may have unfettered access to sensitive data, as well as the means, methods and motives to access information, virtually undetected.

The results of the SANS survey on insider threats show that organizations are starting to recognize the importance of protecting against the insider threat but struggle to deal with it; as one might expect, larger organizations are more likely to have provisions for responding to such threats.

Key findings include:

Insider threats are on IT's radar. Almost three-quarters (74%) of respondents are most concerned about negligent or malicious employees who might be insider threats. The FBI and Department of Homeland Security agree that insider threats have increased and that such threats pose a serious risk.[1]

Organizations fail to focus on solutions. The pattern of survey respondents recognizing the problem while failing to implement solutions that effectively deal with it does not bode well. This yawning gap between claimed priorities and resources available for budget and planning is a playground for attackers.

About a third of organizations know they've experienced an insider attack. This is only the tip of the iceberg; many insider threats go undetected, and some are only detected by accident.

Prevention is more a state of mind than a reality. Over 68% of respondents consider themselves able to prevent or deter an insider incident or attack. Half (51%) believe their prevention methods are "effective" or "very effective." Yet 34% of respondents indicated that they have still suffered actual insider incidents or attacks, some of which were costly.

The financial impact is significant. Almost one-fifth (19%) of respondents believe that the potential loss from an insider threat is more than $5 million; another 15% valued such loss at $1 to $5 million. Immeasurable costs include brand and reputation damage and related costs not tracked in this survey.

[1] *"2014 US State of Cybercrime Survey," Carnegie-Mellon University, Software Engineering Institute, page 7; http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf*

Spending on insider threats will increase next year.
One-fifth (20%) of respondents indicated they will increase their spending on the issue to 7% or more next year, demonstrating more awareness and focus on this area.

The survey also showed how organizations approach insider threats, and this report includes our recommendations for improving incident response (IR), based particularly on these observations:

- ✓ Most respondents focus on nontechnical controls and awareness.
- ✓ Malicious insiders are a greater concern than accidental insiders are.
- ✓ Attack detection takes too long.

With this information, readers should be better prepared to address the threats insiders pose.

Survey Respondents

The survey was open between December 2014 and January 2015; 772 people responded in full to it, a number that suggests the overall importance of and interest in the topic of insider threats. The respondents represent a broad set of industries; **Figure 1** shows the breakdown.

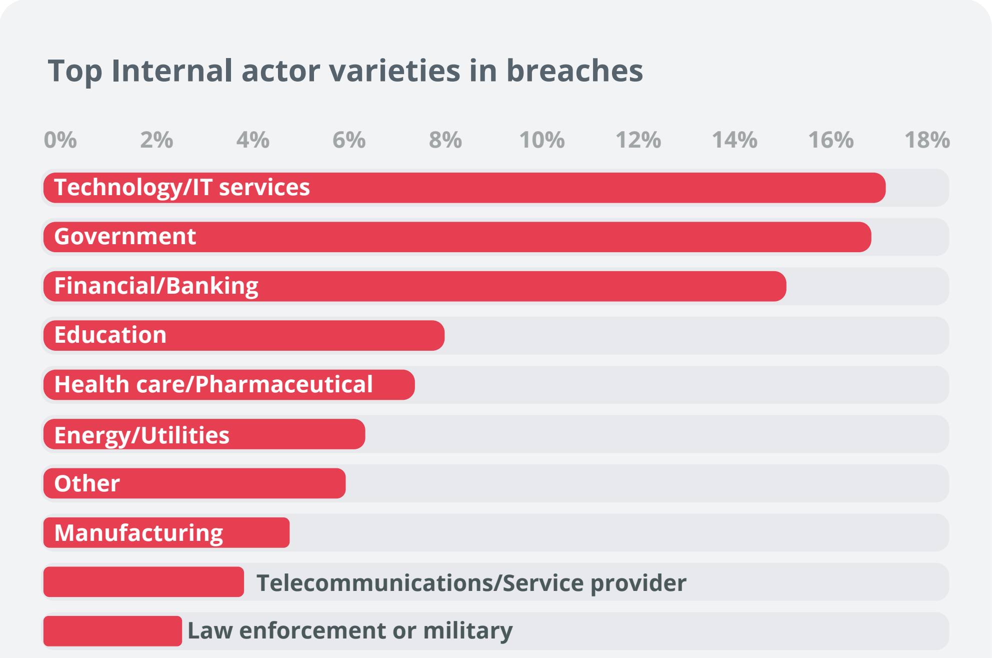


Figure 1. Breakdown of Respondents by Industry

Respondents also represent a wide range of organization sizes, illustrating that neither size nor lack of it can protect an organization from insider threats. The existence of likely target vectors is a better indicator that an attack is feasible than an organization's size or its industry.

Smaller organizations often have feebler security and less detection capability than larger organizations. Because more than half of the respondents work in organizations with workforces smaller than 5,000, this could skew some of the results of questions referring to detection and number of breaches, since smaller organizations often do not detect attacks until they are well under way. **Figure 2** shows the breakdown of organization size.

What is your organization's size in terms of its overall workforce, including employees and outside individuals such as contractors, consultants and interns?

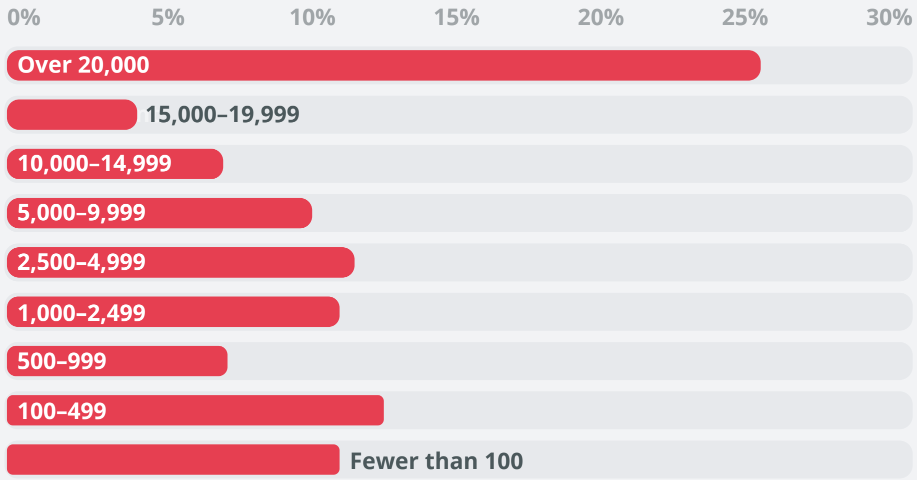


Figure 2. Distribution of Organization Size

Although slightly less than half of the respondents work as security analysts or security management (47%), this changes when comparing the responses to organization size. Respondents from organizations with fewer than 500 users were far more likely to be in general-purpose system administration or IT management jobs than in security-specific roles, doubtless reflecting the leaner IT staff count of such organizations.

Beyond these roles, the respondents hold a diverse set of job titles, including compliance and help desk. This further illustrates the impact that insider threats have on an organization. It is not just a security problem; every business and area of a business has to address and deal with this problem. **Figure 3** shows the roles our respondents most frequently reported holding.

What is your primary role in the organization?

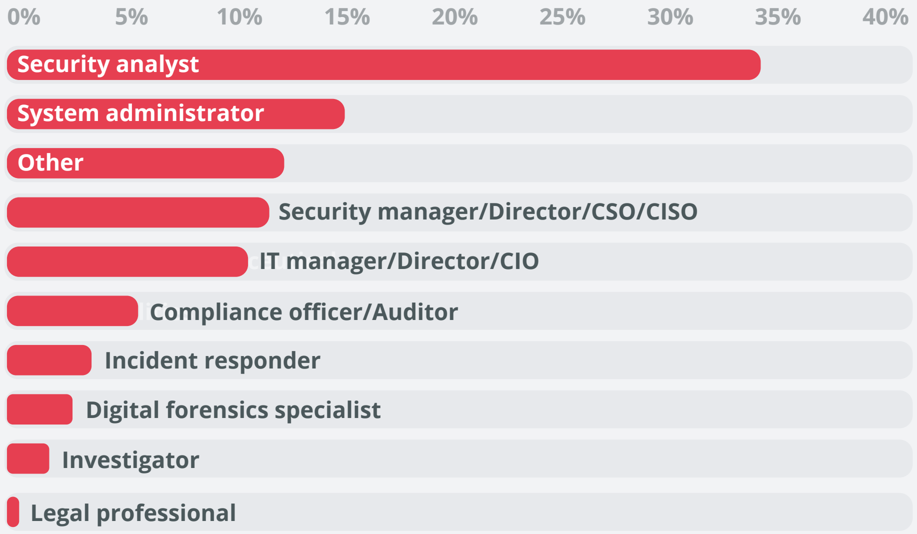
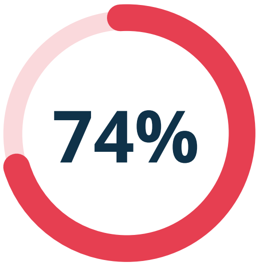


Figure 3. Roles Held by Survey Respondents



Percentage of respondents who were most concerned by the threat from negligent or malicious employees

Assessing Your Vulnerability to Insider Threats

IT organizations should ask the following questions:

- ✓ What information would an adversary target?
- ✓ What systems contain the information that attackers would target?
- ✓ Who has access to critical information?
- ✓ How would an adversary target that individual?
- ✓ What would be the easiest way to compromise an insider?
- ✓ How would someone extract the information?
- ✓ What measures or solutions can IT use to prevent these attacks?
- ✓ What measures or solutions can IT use to detect these attacks?
- ✓ What gaps exist in how we are dealing with insider threats?
- ✓ What are the highest-priority items to focus on?
- ✓ Does our current budget appropriately address insider threats?
- ✓ Should we adjust current resources and budget to address insider threats?
- ✓ What would a security roadmap that includes insider threats look like for our organization?

Categories of Insider Threat

Two broad categories of insider threat exist: the malicious and the accidental. Malicious insiders make a conscious decision to deliberately cause harm to an organization; they are fully aware of their actions and recognize the damage or impact it can have on the organization.[2]

In contrast, accidental insiders are targeted by adversaries and manipulated to do something that the insiders believe to be legitimate but that in reality represents a threat to the organization. Such insiders often have no idea that what they are doing is harmful, and people in this category might simply be negligent (as the responses were phrased) in their security practices or lead to breaches through improper handling of data, systems and networks.

The survey further broke out various classes of insiders to determine whether respondents were most concerned with employees, contractors, customers and clients, or other categories of both malicious and accidental insiders. **Figure 4** shows the breakdown of the responses.

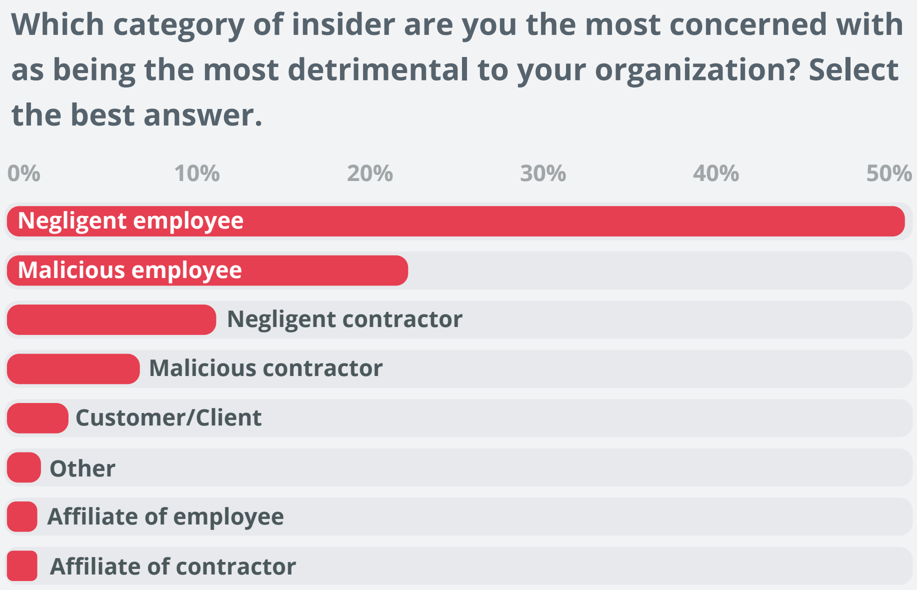


Figure 4. Breakdown of Insider Threats

[2] *This survey did not examine the potential external attacker who, for example, uses compromised credentials to gain access.*

Although malicious or deliberate insiders will always represent a threat, negligent employees are by far the biggest threat to an organization, according to our respondents, with 52% noting it as the biggest concern. These kinds of insiders can include those who simply have poor security processes and those who might be unknowingly manipulated.

Almost 22% considered malicious employees the threat of greatest concern, while 17% placed negligent or malicious contractors first. These numbers directly reflect an organization's ability to detect insider threats and respond appropriately. Because malicious employees cause their harm directly, they give themselves away more readily than accidental or negligent insiders do.

Yes, This Means You Too

Many organizations design their networks in a way that enables accidental as well as malicious insiders to cause significant damage. For example, if an attacker compromises an internal system in a network with a "flat" architecture, he often has visibility into all systems within the organization. Better segmentation and system solution could control potential damage.

Although it may be comforting to believe that insider threats only affect certain organizations or types of businesses, such threats are a systemic problem; any organization is vulnerable to an insider threat, and adversaries will always find the easiest path through an organization's defenses. As organizations improved the protection of their outward-facing systems, adversaries sought an easier way to compromise an organization; targeting insiders proved fruitful. Since many organizations have a relatively flat network, one insider can provide significant access to any information or systems an adversary would want to access.

Concerns, Consequences and Costs

No matter their business, organizations must protect not only their customers' personally identifiable information, but also confidential business information and intellectual property. Moreover, most organizations now recognize the value of protecting their reputations, with the implications of recent breaches at blue-chip retailers and others in mind.

The survey found that 67% of respondents were most concerned about compromising personally identifiable information (whether customer or client), while 54% expressed concern about damage to their reputation stemming from negative publicity around a breach or leak.

Another 51% noted concern over revealing confidential business information (e.g., financial information, customer lists or transaction history), and 44% were worried about losing intellectual property. **Figure 5** shows the concerns most felt by survey respondents.

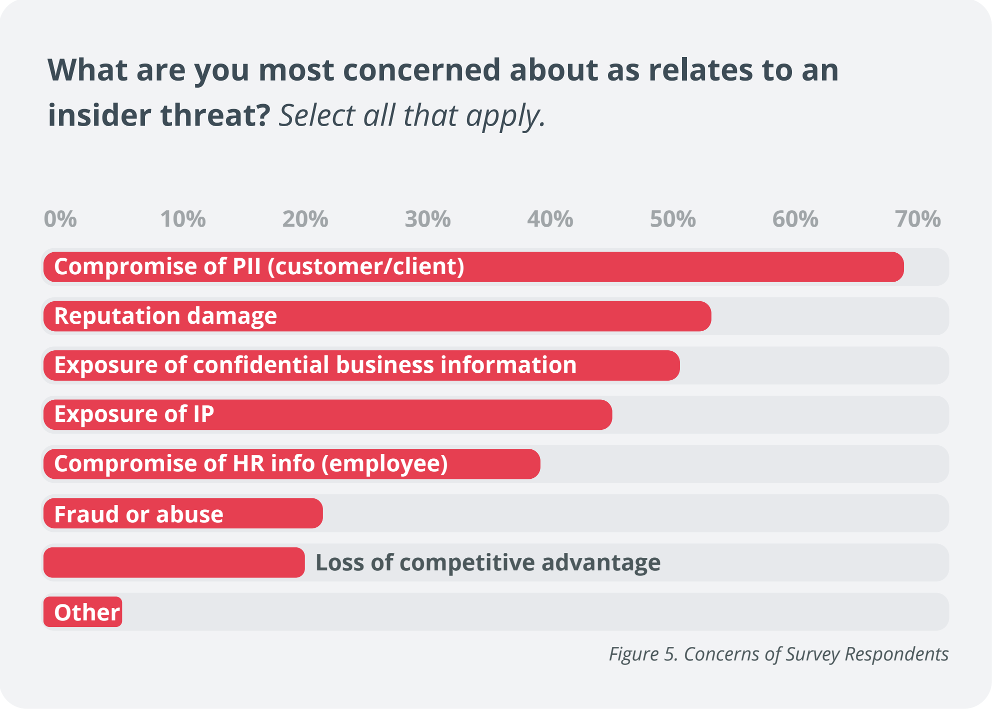


Figure 5. Concerns of Survey Respondents

Interestingly, only 21% feared a loss of competitive advantage, perhaps because the amount of information available online makes competitive analysis much easier than ever.

Comparing these results to respondents' industries produced unsurprising results. For example, customer or client PII compromise was the most frequently reported concern for five of the six most represented industries (education, financial, government, health care and pharmaceutical, and technology services), while respondents from the energy industry were less likely to cite this—due perhaps to the nature of the business. Meanwhile, respondents from financial services and technology businesses were less concerned by reputation damage—otherwise the second most-reported concern of respondent from these six industries—than they were by exposure of confidential business information.

Financial Consequences

Most organizations will feel the financial impact of an insider attack, according to survey results. Our survey respondents anticipate suffering financial losses in the wake of an insider attack ranging as high as millions of dollars, as noted in Figure 6; to our utter lack of surprise, 52% of respondents indicated that they had no idea at all what the losses might be.

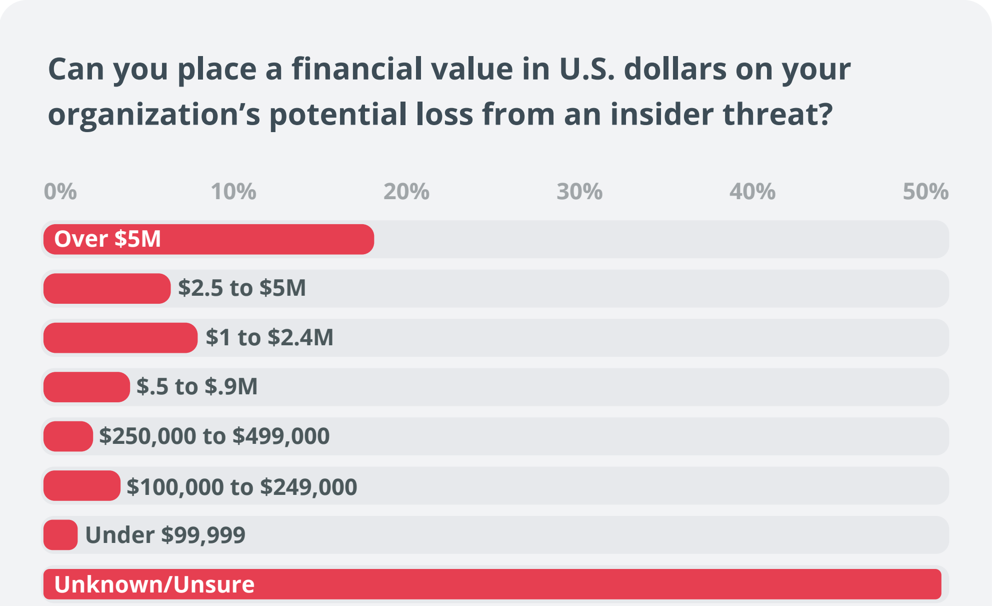


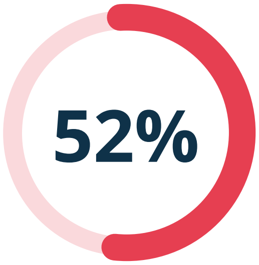
Figure 6. Potential Losses from Insider Threat

Almost one-fifth (19%) of respondents believe that the potential loss from an insider attack would total more than $5 million, an amount in line with what other research has shown is actually being incurred; for example, Ponemon Institute reported in 2014 that the average consolidated total cost of a data breach increased 15% in the preceding year, to $3.5 million.[3] (Of course, this does not differentiate between insider and external attacks, but it does offer support for a trend of growing cost.) The 2014 Verizon Data Breach Report also notes a disturbing trend: for incidents tracked in that report, 72% of insider motives involved financial gain.[4]

The message here is clear: information subject to insider threat has value, even if it is challenging to assign a specific dollar amount, and information is being taken for some very specific financial reasons. We also recognize that it is difficult to measure the true cost of an insider threat because of the time required to identify and neutralize the threat.

Budgeting to Address Insider Threats

Since most organizations do not have a separate budget item for insider threat countermeasures, it's not difficult to imagine why 47% of the respondents lacked specific knowledge of their spending on insider threats. After all, organizations usually base their budgets on where they spend money, rather than the problems the money solves. Typical security budgets have line items for firewalls, IPSes or DLP, but do not have money allocated for "threat prevention."



Percentage of respondents who have no idea what losses from insider threats might total

This suggests that organizations spend little if any dedicated resources on insider threats. Because such threats are a problem that has been recognized relatively recently, we accept that organizations do not yet have any dedicated line items for this area. Based on the results of this survey, respondents show that this is a growing concern and that insiders are constant targets. As with any problem in security, organizations absolutely must dedicate resources to this problem or it will continue to get worse.

[3] *"Global Cost of Data Breach Increased by 15 percent, According to Ponemon Institute," Ponemon Institute press release, May 5, 2014; www.ponemon.org/news-2/58'*

[4] *"2014 Data Breach Investigations Report," page 24; www.verizonenterprise.com/DBIR/2014*

Figure 7 shows the share of the IT budget respondents allocated to dealing with insider threats.

What percentage of your IT budget are you currently spending for prevention and detection of insider incidents/attacks?
What do you estimate this percentage might be in the next twelve months?

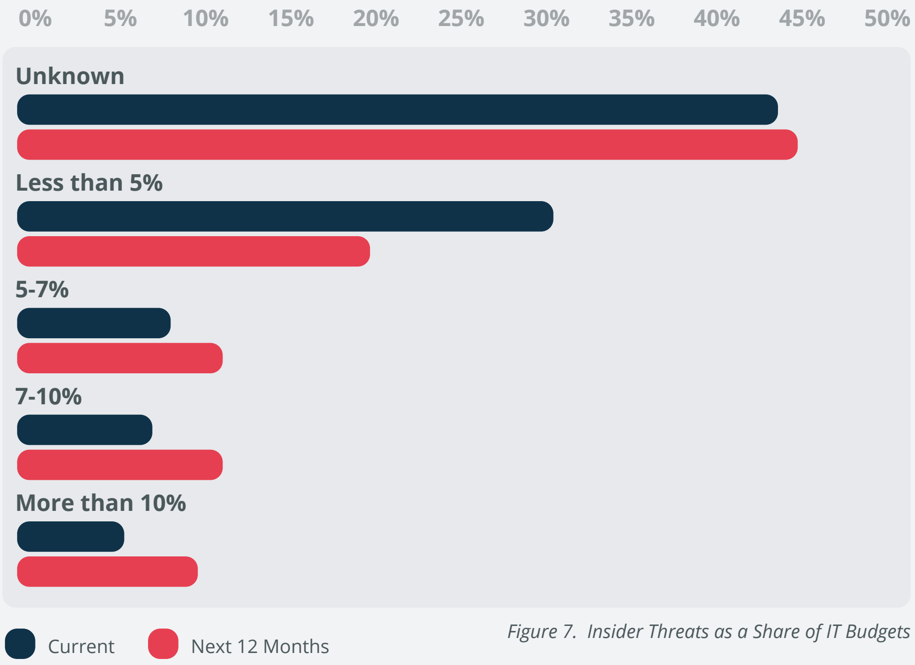
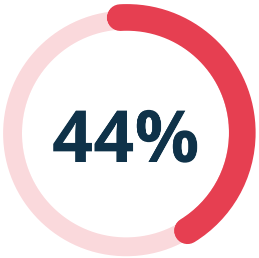


Figure 7. Insider Threats as a Share of IT Budgets

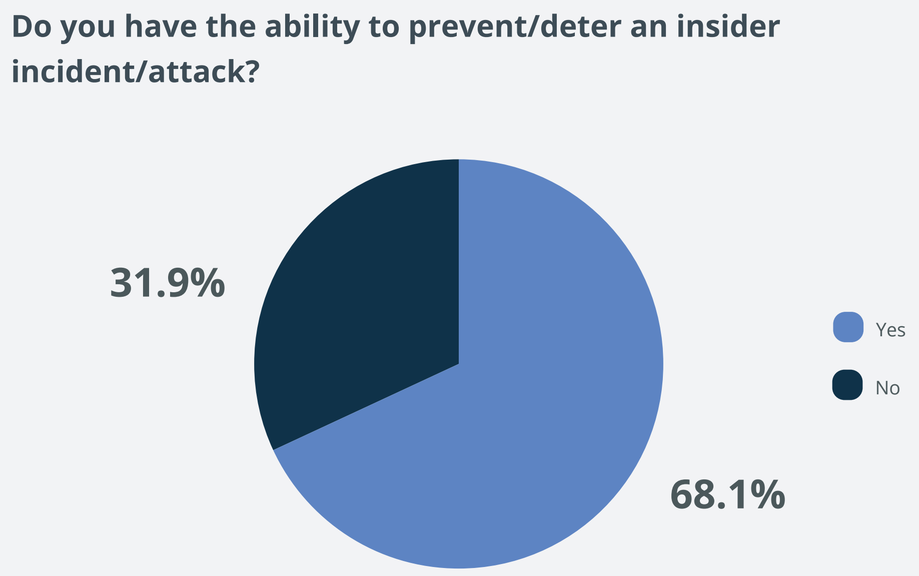
A look at the survey results shows that most organizations have a similar budget misalignment, which goes a long way toward explaining why insider threats continue to be a major problem for IT. As noted earlier, more than half (52%) of respondents perceive negligent employees as the cause of significant damage, while almost half (44%) are spending 10% or less of their budget on this area, so it's clear why survey respondents also suffer a significant number of insider breaches.



Percentage of respondents who are spending 10% or less of their IT budget on insider threats

Preventing Insider Threats

Our survey asked practitioners to assess their ability to prevent or deter insider incidents and attacks. **Figure 8** shows respondents are quite confident in this area.



Do you have the ability to prevent/deter an insider incident/attack?

Figure 8. Ability to Prevent Insider Incidents and Attacks

Naturally, organizations attempt to prevent attacks or stop the damage before it occurs, but advanced attacks and insider threats make prevention difficult; in most cases, damage control begins with detection. With 68% of respondents believing they can prevent attacks, many organizations still focus on basic insider threats (i.e., negligent users) without realizing how many attacks they miss. In fact, 75% of insider crimes go unreported or are not prosecuted, and 36% of companies cite lack of evidence as a reason why.[5]

Most organizations will suffer an insider compromise and many will be unable to prevent all attacks. That your organization currently has an insider threat of some sort is a near certainty. Therefore, you have to approach security with the assumption that an insider threat has already compromised you and focus your energy on detection.

[5] *"2014 US State of Cybercrime Survey," Carnegie-Mellon University, Software Engineering Institute, page 7; http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf*

Preventing insider attacks is important and a key part of security; however, organizations often fool themselves into believing that they can stop all such attacks. Repeat the following sentence three times: “Your organization is and will be compromised by insiders.” Insiders—whether malicious or merely negligent—are a continuous and constant problem for IT security; thinking otherwise is naïve.

Tools and Techniques in Use

Because they perceive insider threats as a “people” problem, many organizations rely heavily on administrative solutions such as policies and procedures to deal with the problem. Indeed, an overwhelming share of respondents (90%) say they utilize these techniques, but any effective solution must integrate people, processes and technologies. Administrative solutions cover people and processes, but without technologies to monitor compliance and enforcement, those solutions often fall short.

As we will see, 34% of respondents indicated that they have suffered actual insider incidents or attacks, some of which cost their organizations millions. If these same organizations are using administrative controls as their main defense against insider threats, this could indicate that such administrative policies and procedures are partially ineffective, at least for these respondents.

Although policies and procedures remain critical to security, technical solutions that address prevention, detection and deterrence can effectively augment the controls implemented to counter insider threats. **Figure 9** shows that the respondents prefer policies, audits and monitoring to deal with insider threats.

What tools or techniques are you using to prevent/deter insider threats before they become an actual incident or attack?

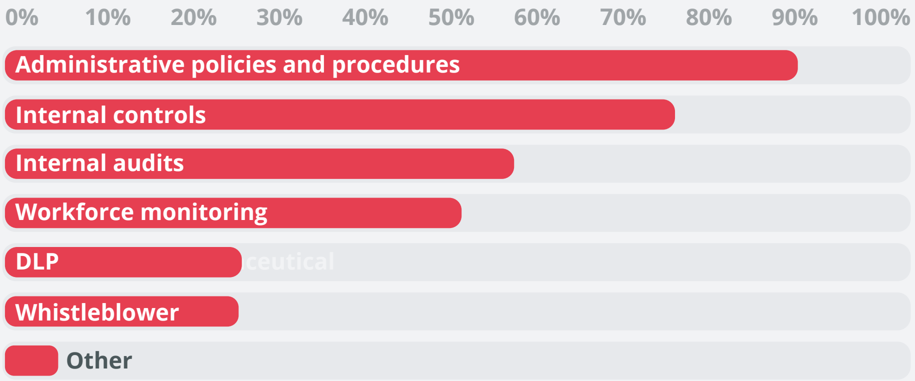


Figure 9. Tools and Techniques Used to Prevent or Deter Insider Threats

Use the Tools You Already Have

Although insider threats are not an easy problem to solve, technical solutions exist that organizations can use to reduce the risk, including

- Inbound and outbound proxies
- Content filtering and sandboxing of executables
- Application whitelisting
- Web filtering and content blocking
- Data classification
- Data loss prevention (DLP) with data flow analysis
- Netflow analysis to detect data exfiltration
- User activity monitoring (UAM)
- SIEM systems or other log-focused tools for detecting anomalies in user patterns

Although organizations may possess many of these tools, they often are not configured to detect or deter insider threats. Combating insider threats does not always require purchasing new solutions; it may simply mean analyzing what you already have and tuning it to focus on the problem.

Our respondents' declared reliance on "soft" solutions illustrates a gap in how organizations perceive insider threats, and this list can help fill that gap. Insider threats are an advanced attack vector that requires an integrated defense-in-depth strategy.

Obstacles to Prevention

The biggest challenge with insider threats, based on SANS training and analysis, is that organizations have not focused resources on this problem—or they simply are not prioritizing it. Therefore, when asked what factors are limiting an organization's ability to deal with insider threats, many respondents blamed multiple factors.

Lack of training was a leading factor for 51% of respondents, followed by lack of budget, at 43%. The other most-cited factors were lack of staff (40%), lack of technology solutions (40%) and lack of appropriate policies and procedures (32%). This last is interesting, because 90% of respondents had claimed to rely on such policies and procedures in the previous question. Although policies and procedures are important, they form the basis of a solution but are not a solution by themselves; technology must augment them.

Dismayingly, 28% of respondents said that preventing or deterring insider threats was not a priority for their organization. That response suggests an organizational attitude that awareness and training could address. Because corporate cultures flow from the top, it is important that the executive team understands and appreciates the damages insider threats can cause, so that this awareness can spread throughout the organization.

Figure 10 shows the breakdown of responses to this question.

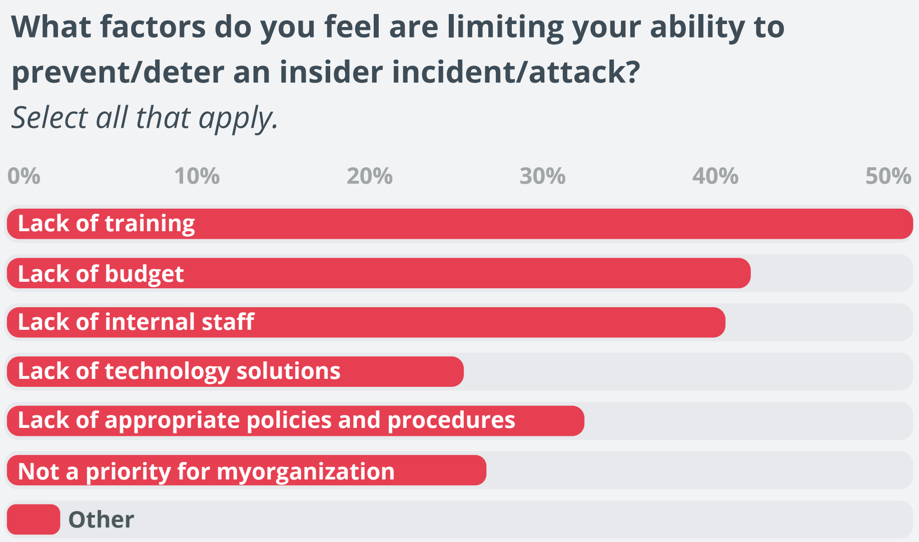


Figure 10. Factors Limiting Prevention or Deterrence

Looking at these results based on organization size, lack of budget, staff and training remain the top three issues for respondents from medium-size organizations (1,000–9,999 users); those from larger and smaller organizations were more likely to report lack of technology solutions in their top three, with lack of staff being pushed into fourth place.

Prevention versus Detection

We next asked respondents about the effectiveness of their prevention measures. Only 9% believe they have proven tools or techniques against an attack, while 42% are confident they have selected the best tools or techniques—but have not used them operationally. A frightening 36% assessed their prevention measures as not effective, a figure that is more understandable when you consider that many common preventive devices (e.g., firewalls and IDS/IPSes) only defend against threats from the outside. Devices focusing on external threats will have minimal impact against internal threats and organizations should augment these with products specifically designed to defend against insider threats.

Figure 11 shows the respondents' self assessment of the effectiveness of these prevention measures.

What's Your Insider Threat GPA?

The responses indicate that respondents feel they are coming up short in multiple areas when it comes to addressing insider threats. We recommend an integrated solution across people, processes and technology. Insider threats require a comprehensive solution that ties in all areas of the business. To help determine the biggest gapsin your organization, draw up a report card. In the following areas, give yourself an "A" if you are addressing that area, an "F" if you are ignoring it, and intermediate grades as appropriate:

- ✓ Policy
- ✓ Procedures
- ✓ Awareness
- ✓ Training
- ✓ Technology
- ✓ Administrative
- ✓ Executive support

By calculating your "insider threat GPA," you can see what the biggest exposure you have to insider threats is likely to be.

How effective do you feel your prevention measures are?

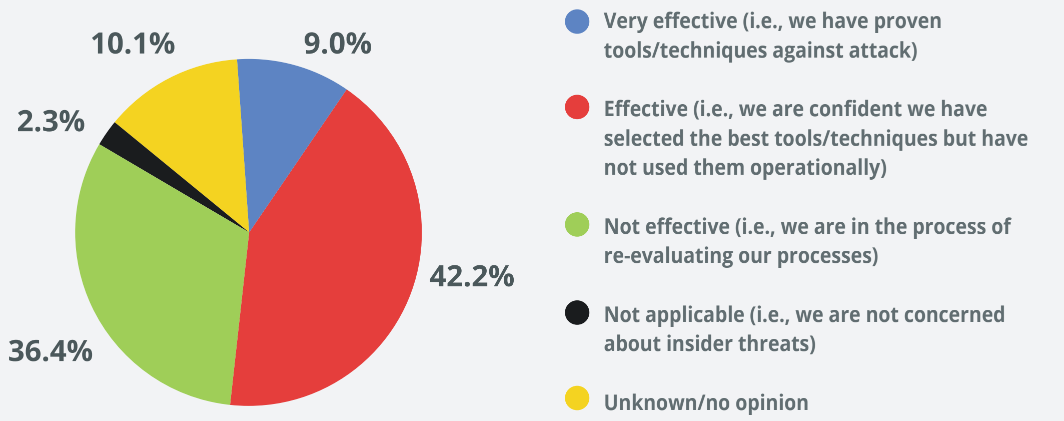


Figure 11. Effectiveness of Prevention Measures

Because the insider already has internal access, accounts and corporate assets, the primary focus for effectively dealing with insider threats is detection. We will look at the tools respondents use and which they find effective in the next section.

As we've noted throughout this paper, organizations have to assume that the insider threat is not only real, but also active and present. This is where detection and response come into their own. Detecting insider threats requires visibility into actions that users and applications perform, identifying deviations in normal behavior and using that information to identify distinct threats. Audits, monitoring and log analysis are all essential parts of the detection of insider threats.

The fact that organizations are investing in detection is a positive sign, since it will give the best return on the money spent to uncover insider threats. It is important to note that any technological solution must be correctly designed, properly configured and appropriately deployed. **Figure 12** shows the tools and techniques used by our respondents when detecting insider attacks and incidents.

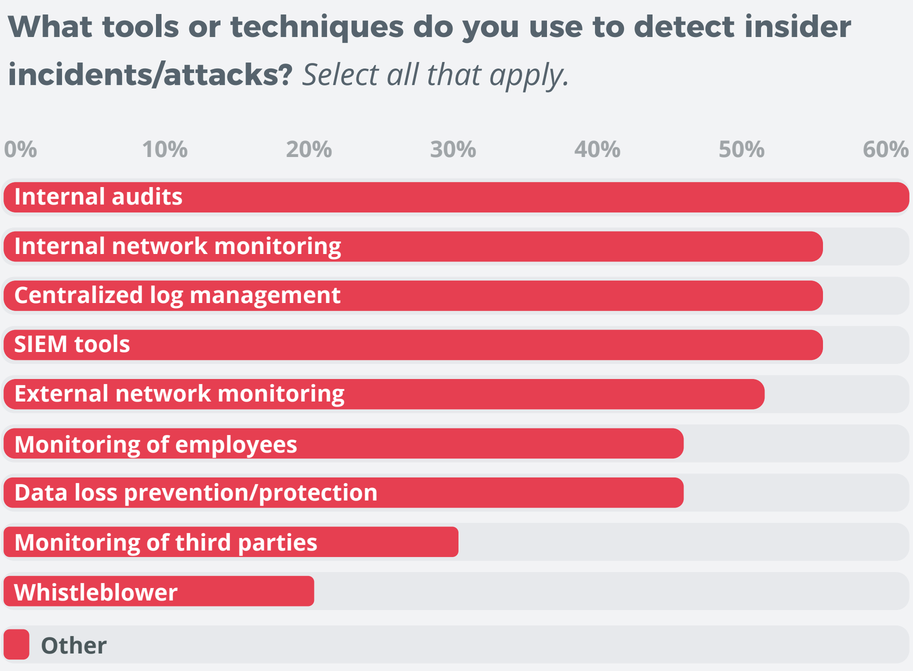
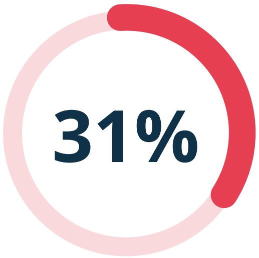


Figure 12. Tools and Techniques Used to Detect Insider Threats

Internal audits (61%), internal network monitoring (57%), centralized log management (57%), SIEM tools (55%), external monitoring (52%), employee monitoring (47%) and DLP (45%) led the pack of potential solutions.

Properly implementing a solution calls for two key components: people and dollars. If the organization already lacks people to implement and maintain the solutions, simply buying a box with flashing lights or software with a nifty dashboard will not solve the problem. The most effective detection requires 24/7 monitoring and analysis of the resulting data.



Percentage of respondents who have no formal IR plan or are unsure whether one exists

Incident Response Plans

Encouragingly, 69% of respondents said they have an incident response (IR) plan, but the bad news is that just over half of those plans do not include any specific provisions for insider threats. Unfortunately, 17% of our survey takers have no IR plan in place, and almost as many don't even know if they have a plan or what it contains, as we see in **Figure 13**.

7

Does your incident response plan have special provisions for incidents involving insiders?

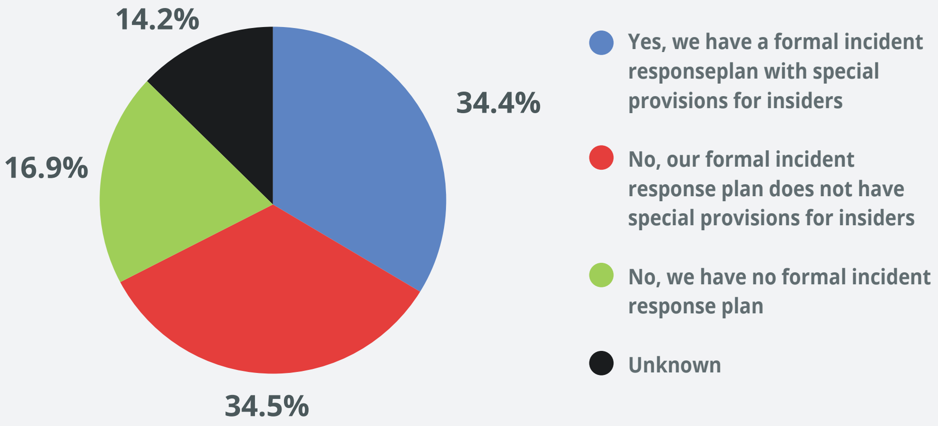


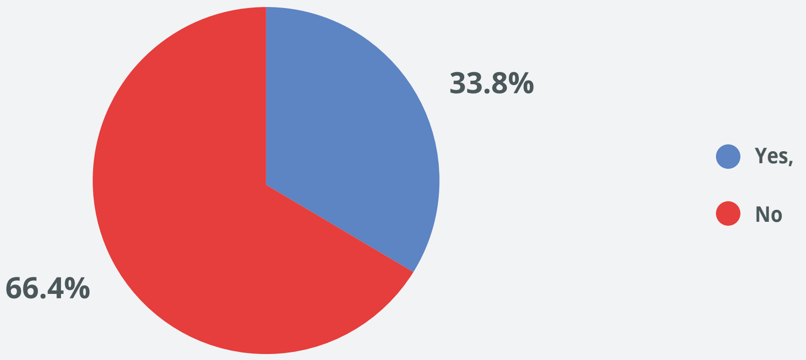
Figure 13. IR Plans and Provisions for Insider Incidents

IR matters because it directly controls the damage and impact an incident can have on an organization. A plan that addresses internal as well as external threats will enable timely response and mitigation. Without such a plan, the amount of damage and exposure from an attack can be significantly worse than if it was controlled and managed.

Larger organizations (more than 10,000 users) were almost twice as likely to report having provisions in place against insider threats as smaller outfits (fewer than 1,000 users) were; interestingly, the results for medium-size organizations tracked those from the smaller ones much more closely than they did those of the larger shops.

Experience of Insider Threat Incidents

So, given the potential financial and business impact of a successful insider attack and the level of preparedness the respondents claim, who actually has been attacked? Roughly, one-third (34%) of survey respondents have experienced an insider incident or attack, as we see in **Figure 14**.



Does your incident response plan have special provisions for incidents involving insiders?

Figure 14. Experience of Insider Incidents or Attacks

That leaves 66% who say they have not experienced such an attack; while that is possible, it is equally likely that these respondents believe they've escaped attack, but haven't—they just don't know the attack happened. If you have not detected an incident, you may not be looking in the right place; alter your game plan by looking in different places in your logs or adding tools that focus on insider threats.

Detecting and Mitigating: How Time Flies

The time our respondents required to detect an insider incident or attack ranged from less than an hour to more than a year, with 24% saying this information was unknown; only 10% detected such incidents in less than an hour. Time to mitigate followed a similar range; Figure 15 shows the breakdown of responses for each stage.

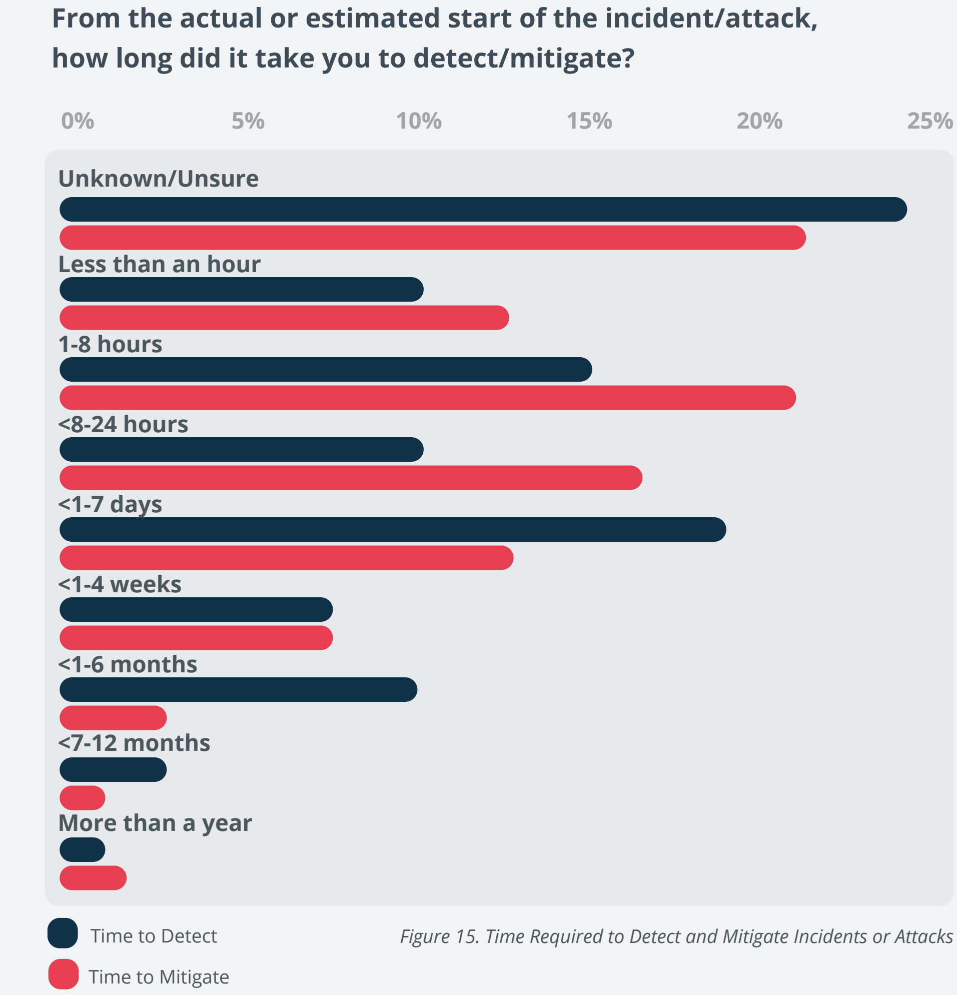
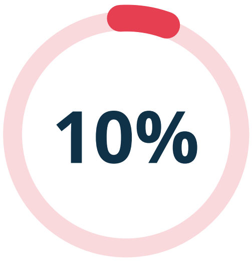


Figure 15. Time Required to Detect and Mitigate Incidents or Attacks

Because such a large number of respondents don't know the time they need for detection or mitigation, our advice is to think like the adversary: if you were a malicious insider, how would you go about stealing and causing harm to your organization? Based on this analysis, start looking in those areas for signs of compromise.)



Percentage of respondents who detected insider attacks within an hour

A key component of detection is log correlation and analysis. Security incident and event management (SIEM) tools that enable log correlation are vital when combating the insider threat and when used with other solutions. SIEM tools are only as good as the data that you provide them; they must receive data on user activity to be effective against insider threats. The closer you can get to the actual user and point of action, the more effective your analysis will be.

Table 1 shows the detection and response times for respondents from the top six industries in our survey.

7

Table 1.
Detection/Response for Respondents with Insider Breaches

Industry	Time to Detect (Days)	Time to Respond (Days)
Education	22.53	0.78
Energy/Utilities	11.90	25.40
Financial/Banking	47.94	11.66
Government	48.03	59.40
Health care/Pharmaceutical	30.01	24.01
Technology/IT Services	40.11	5.26

Respondents from government proved slowest in detecting breaches and reacting to them, while survey respondents from education moved with alacrity once they knew of the breach.

Damage Assessment

The responses to a question asking respondents to estimate the cost of their worst loss show that insider threats can cause financial damage to organizations. However, as we have seen from other data from this survey, many organizations lack advanced detection capabilities and might only find low-end, unsophisticated attacks—or not detect them at all. Figure 16 shows the breakdown of responses.

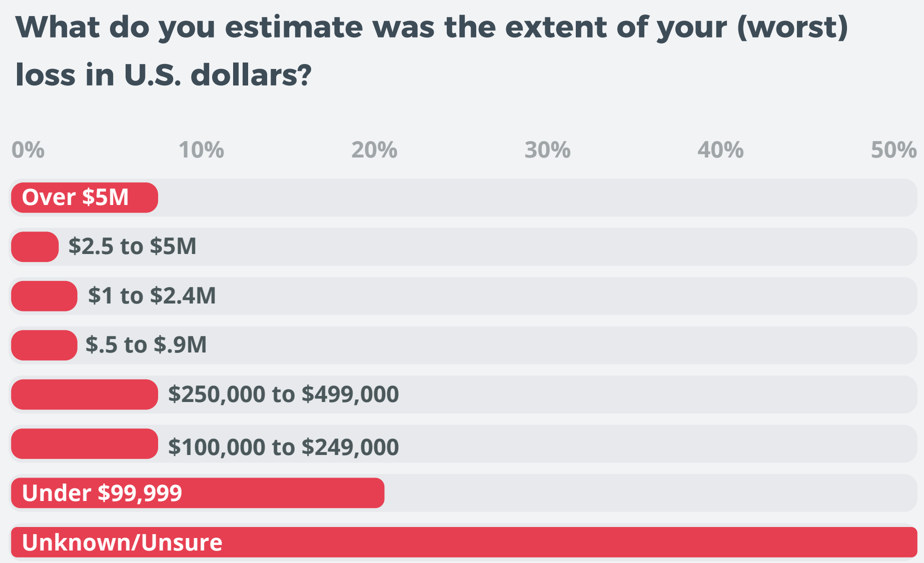

What do you estimate was the extent of your (worst) loss in U.S. dollars?

Figure 16. Damage Estimates

Even this limited data indicates that, for the respondents experiencing a minimum of $5 million in losses, the combined losses are more than $231 million.

Conclusion

Insiders have access to critical information, understand how the organization is structured, and can bypass security more easily than outsiders. They can therefore be in the best position to cause harm to an organization. A main theme of the survey results is that organizations increasingly recognize the danger posed by insider threats. However, the survey also shows that many organizations are still not creating and implementing insider threat programs and need to aggressively increase their focus to better protect the organization. Essentially, organizations recognize the damage of insider threats but are doing too little to directly address the exposure and harm they can cause.

Organizations should perform these steps to better address the insider threat:

- ✓ Perform damage assessment of threats
- ✓ Map past and current investments against threats
- ✓ Determine exposure to insider threats
- ✓ Create attack models to identify exposures
- ✓ Identify root-cause vulnerabilities
- ✓ Block and remove the vector of the attack
- ✓ Control flow of inbound delivery methods
- ✓ Filter on executable, mail and web links
- ✓ Monitor and look for anomalies in outbound traffic

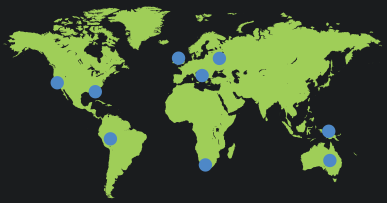
Furthermore, they need to take aggressive steps to implement administrative and technical solutions for controlling the damage an insider can cause.

About the Author

Dr. Eric Cole is a SANS Faculty Fellow and an industry-recognized security expert with over 20 years of hands-on experience in information technology, focusing on helping customers build dynamic defense solutions that protect organizations from advanced threats. Dr. Cole has a master's degree in computer science from the New York Institute of Technology and a doctorate from Pace University with a concentration in information security. He is the author of several books, including Advanced Persistent Threat, Hackers Beware, Hiding in Plain Site, Network Security Bible, and Insider Threat. He is credited on more than 20 patents; is a researcher, writer and speaker; and is also a member of the President's Commission on Cyber Security and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting and has served as CTO of McAfee and chief scientist for Lockheed Martin. He is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware.

To learn more about how Veriato can help you with **Insider Threats & Rapid Response,** contact a Veriato representative today.

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA

4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA

3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL   United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/