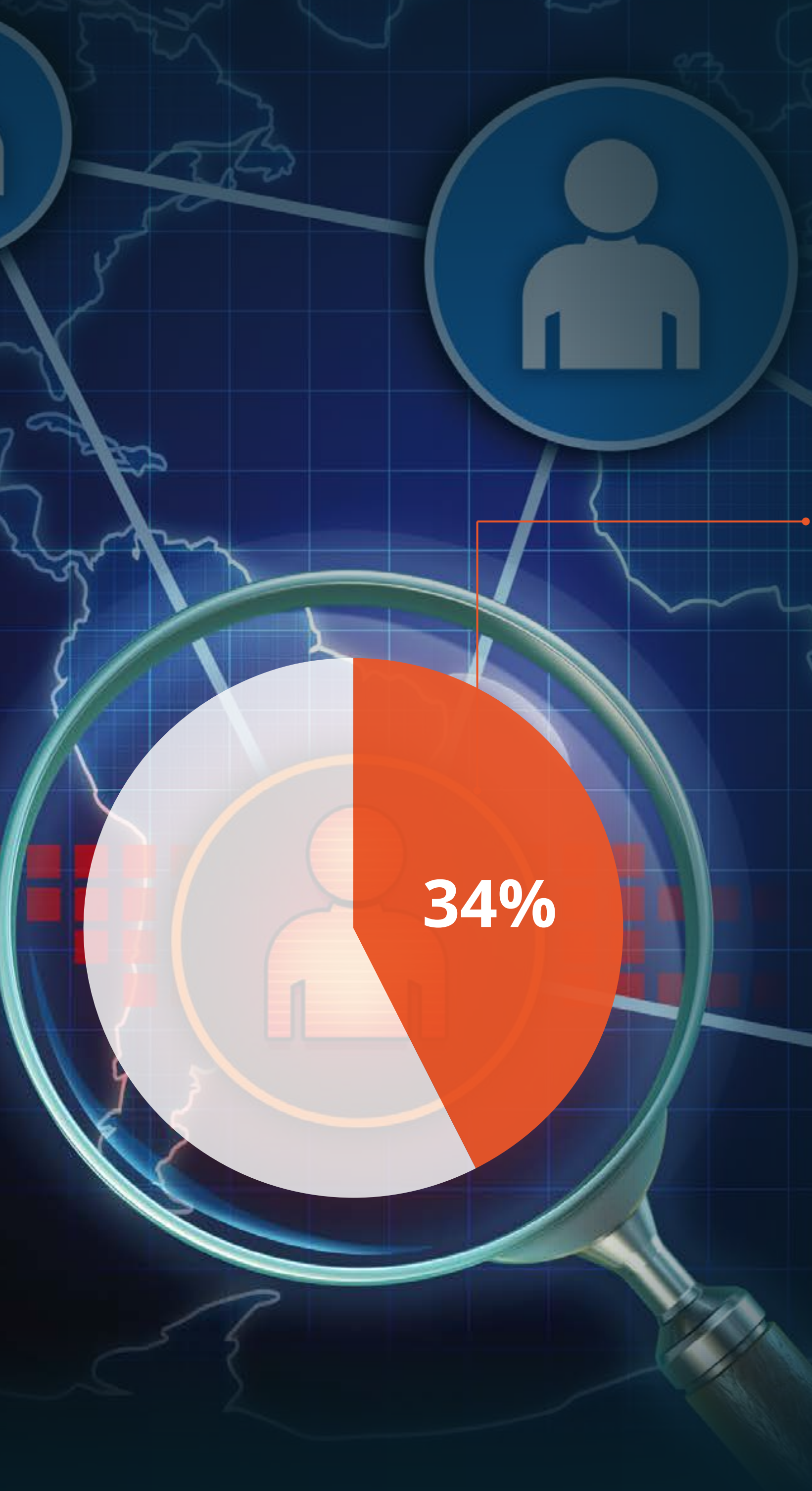
The Guide to Budgeting for Insider Threat Management

observe it

The Guide to Budgeting for Insider Threat Management

This guide is intended to help show you how to approach including Insider Threat Management within your cybersecurity budget planning. The guide looks at current budgetary trends, top cost centers, best practices in risk evaluation, and various approaches to developing your own insider threat budget.



A recent study from The Ponemon Institute shows the average global, annual cost of insider threats is now $8.76 million. For the study, researchers spoke with 717 IT and IT security practitioners.

34% of the respondents reported that a lack of budget was a major barrier to effective insider threat management — which is ironic, given the rising costs of insider threat prevention, detection, and response.[1] (Not to mention the increasing number of high-profile incidents reported on by the news media.)

Organizations need to think about insider threat budgeting holistically. It should be considered part of their overall cybersecurity strategy. For example, you wouldn't attempt to create a budget for a home renovation without first planning and evaluating the cost of the required materials, including labor for the workers (not to mention the unknown risks that may lie beneath enclosed walls).

[1] https://www.observeit.com/ponemon-report-cost-of-insider-threats/

How much does the response to an insider threat incident cost?
How would the money be spent, and is it a recurring cost?

Budgetary Trends

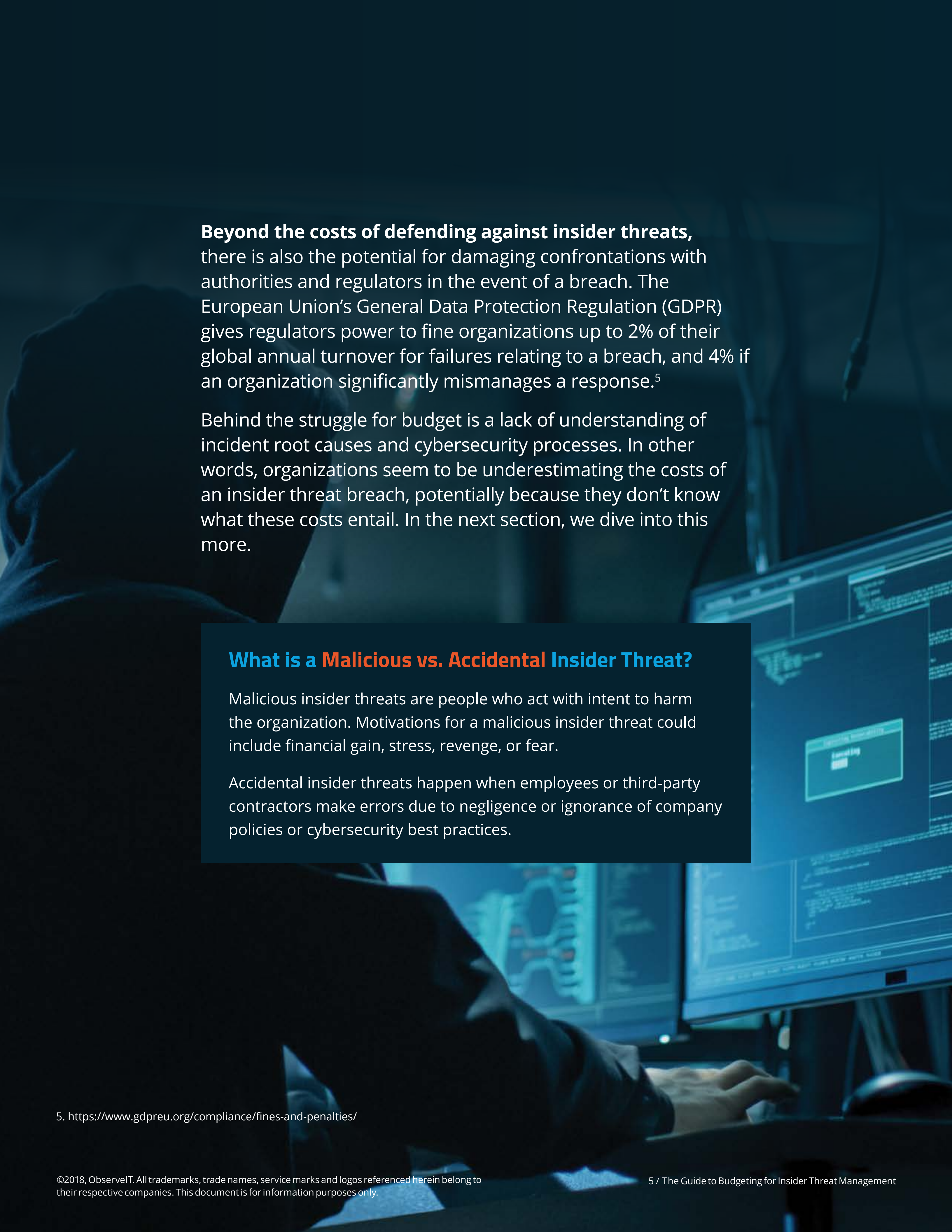
The increased prevalence of cybersecurity threats suggests that teams need more resources — but many organizations struggle to get the budget they need to be most effective. As for the well-funded cybersecurity organizations, work is often still needed to define how a budget is split and allocated among the various threat types.

According to the 20th annual EY Global Information Security Survey (GISS)[2], 87% of organizations say they require up to 50% more funding for insider threats. However, only 12% of organizations expect to receive a budget increase of more than 25% this year.

Unfortunately, for many organizations, the worst may have to happen for them to finally invest in the cybersecurity resources they need. When asked what kind of event it would take to get a cybersecurity budget increase, 76% of survey respondents said a destructive breach would likely result in more resources. Conversely, 64% said if an attack did not appear to have caused harm it would be unlikely to prompt a budget increase.[3] However, history tells us that waiting for disaster is never an effective strategy.

This is bad news for insider threat budgets, too. According to Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey, **28% of organizations have no budget to address insider threats. 16% of respondents said they suspect that their insider threat budget will decrease in the next 12 months.** Organizations that spend 5% or less of their IT budgets on prevention said they plan to spend less on insider threats over the next year, whereas organizations that spend more than 5% on insider threats plan to increase their spending. When asked how the budget was dispersed between malicious and accidental threats, 56% did not know.[4]

2. https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf
3. https://www.marketwatch.com/press-release/organizations-are-at-high-risk-from-cyber-attacks-common-attack-methods-still-successful-ey-survey-finds-2017-11-21
4. https://www.sans.org/reading-room/whitepapers/awareness/defending-wrong-enemy-2017-insider-threat-survey-37890



Beyond the costs of defending against insider threats, there is also the potential for damaging confrontations with authorities and regulators in the event of a breach. The European Union's General Data Protection Regulation (GDPR) gives regulators power to fine organizations up to 2% of their global annual turnover for failures relating to a breach, and 4% if an organization significantly mismanages a response.[5]

Behind the struggle for budget is a lack of understanding of incident root causes and cybersecurity processes. In other words, organizations seem to be underestimating the costs of an insider threat breach, potentially because they don't know what these costs entail. In the next section, we dive into this more.

What is a Malicious vs. Accidental Insider Threat?

Malicious insider threats are people who act with intent to harm the organization. Motivations for a malicious insider threat could include financial gain, stress, revenge, or fear.

Accidental insider threats happen when employees or third-party contractors make errors due to negligence or ignorance of company policies or cybersecurity best practices.

[5] https://www.gdpreu.org/compliance/fines-and-penalties/

Top Cost Centers for Insider Threat

These are logical questions — and depending on the type of incident, the costs could vary greatly.

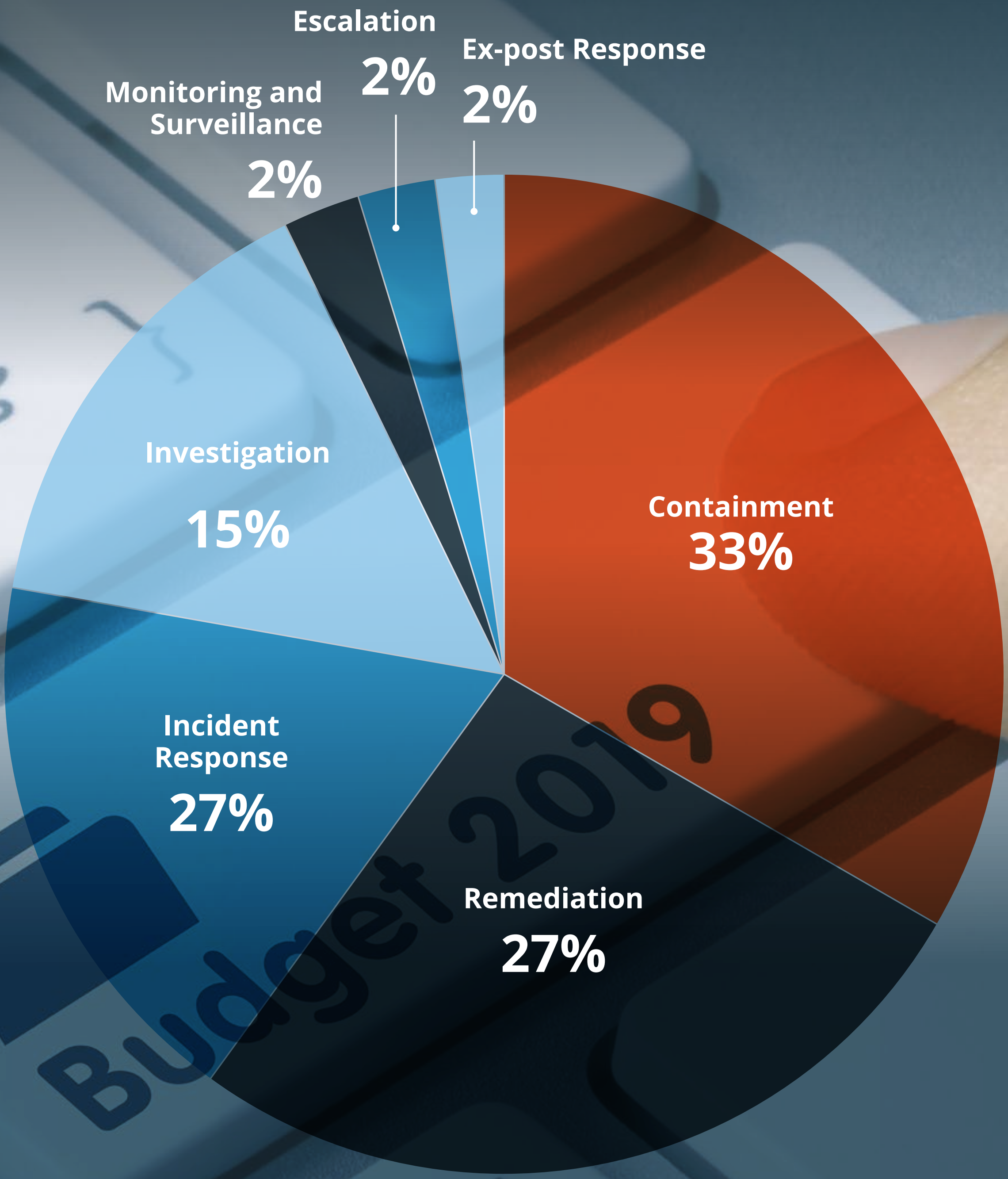
The following table, developed by the Ponemon Institute for the 2018 Cost of Insider Threats: Global Organizations survey report, shows an example activity cost center across three different types of incidents: employee or contractor negligence, criminal/malicious insider, and credential theft.[6] The example framework estimates the total average annualized cost per incident at more than $500,000.

The study addresses the core activities that drive a range of expenditures associated with insider threat response. The cost activity centers include:

2018 ACTIVITY COST CENTERS		EMPLOYEE OR CONTRACTOR NEGLIGENCE	CRIMINAL & MALICIOUS INSIDER	CREDENTIAL THIEF (IMPOSTER RISK)	AVERAGE COST
Monitoring and Surveillance	Activities that enable firms to detect and prevent insider incidents. This includes technologies that enhance mitigation or early detection, such as employee and third-party monitoring.	$16,728	$10,461	$10,712	$12,634
Insider Threat Investigation NSA & Edward Snowden	Activities necessary to uncover the source and scope of an incident.	$41,064	$82,802	$111,328	$78,398
Escalation	Activities taken to alert key stakeholders about incidents and activate an initial response.	$5,533	$19,689	$12,405	$12,542
Incident Response	Activities involving the development and engagement of the incident response team, including an official response from management.	$47,805	$120,857	$105,128	$91,263
Containment	Activities that focus on stopping or weakening the severity of insider incidents or attacks, like shutting down vulnerable applications.	$50,407	$162,816	$305,957	$173,060
Ex-post Response	Activities to help the organization minimize future incidents and data loss prevention. This includes working with internal and external stakeholders to develop an plan that will minimize the potential harm resulting from the threat.	$14,591	$9,987	$9,895	$11,491
Remediation	Activities related to repairing the organization's systems and processes — including the restoration of damaged information and IT infrastructure.	$101,429	$197,480	$116,687	$138,532
TOTAL		**$277,557**	**$604,092**	**$672,112**	**$517,920**

[6] https://www.observeit.com/ponemon-report-cost-of-insider-threats/

The following pie chart shows the percentage cost for seven activity centers. Preventative measures like monitoring & surveillance take up a minimal budget — just 2%. Meanwhile, reactionary activities are the vast majority of expenditures, with investigations taking up 15% of budgets, incident response taking up 18%, and remediation costing 27%.



Evaluating Your Cost of Risk

You only know what you know, and can only detect what you can see. If your organization doesn't have visibility into the potential causes of insider threats, the best you can do is to provide an evaluation to the executive team to help them understand what an incident would cost your organization based on known data, such as the top cost centers detailed above.

Another option is to create holistic cybersecurity risk assessment[7] and identify the areas of greatest risk, ranking them in order of urgency.

For example, how much would it cost to contain and remediate an insider threat incident? Imagine having to take a system offline completely for a certain period of time while an incident is remediated. The business opportunity cost of the downtime, combined with the expense of getting back up and running, could be significant. Add even more cost and time spent on investigation if there are no appropriate tools to give data-backed evidence and context into the incident.

The good news is, you don't have to reinvent the wheel when it comes to risk evaluation. There are certain questions you can use guide the process at your organization. For example, refer to the U.S Department of Homeland Security's recommended list of cybersecurity risk evaluation questions for CEOs:[8]

1. **How is our executive leadership informed about the current level and business impact of cyber risks to our company?**
2. **What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?**
3. **How does our cybersecurity program apply industry standards and best practices?**
4. **How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?**
5. **How comprehensive is our cyber incident response plan? How often is it tested?**

Once you've assessed your risks, it's time to sit down and officially create a budget. In the following section, we'll walk through the key items your team should consider throughout the process.

[7] https://www.sans.org/reading-room/whitepapers/auditing/overview-threat-risk-assessment-76
[8] https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

Creating a Budget That Includes Insider Threat Management

Your insider threat budget should cover both hard costs — like hardware and software technology expenditures — and opportunity costs to develop people and processes.

Technology isn't a silver bullet solution to the problem of insider threats. In reality, an effective Insider Threat Management strategy involves a combination of people, processes, and technology.

To build an insider threat program, you need to select a champion of the program, along with a team of stakeholders to support the initiative. Next comes training and enforcing new processes and technology. Your insider threat budget should cover all three of these areas. Here is what each piece entails from a cost perspective:

People Costs

Includes training technical resources, developing a dedicated insider threat team, and training employees on proper cybersecurity hygiene.

Process Costs

Includes creating an incident response plan and cybersecurity policy, and enforcing those policies and enacting plans on a regular basis.

Technology Costs

Includes the cost of insider threat solutions — plus the cost of taking systems offline and remediating technical issues in the event of a breach.

There are many questions you need to ask yourself when creating a budget that will support people, processes, and technology. This sample checklist can help you get the conversation started with your team:

☐ **What is the financial value of the assets you're trying to protect?**

☐ **What are the risks, beyond financial?**

Lost business, litigation, exposure of trade secrets, and the PR impact of an incident should all be considered.[9]

☐ **What is the likelihood of an insider breach?**

According to the Ponemon Institute, insider threats impact companies of all sizes. All types of insider threat incidents are increasing. Since 2016, the average number of incidents involving employee or contractor negligence has increased by 26%, and by 53% for criminal and malicious insiders. Some organizations are in more danger than others — like financial services firms. The average number of credential theft incidents has more than doubled over the past two years, increasing by 170%.[10]

☐ **Do we have an effective, enforceable cybersecurity policy?**

Do we have the right Insider Threat Management technology? Many organizations make the mistake of investing in security technology without first having properly skilled employees to implement and operate the software, nor the processes to enforce best practices throughout the company. Develop your strategy first before investing budget in a new initiative or tool.

☐ **Do we have a dedicated line of business to insider threat?**

If not, should we pick a current employee to manage that line of business?

☐ **Do we have an incident response plan?**

If not, what is the opportunity cost of developing a plan? (Tip: Insider Threat Management software can help speed up the incident response plan.)[11]

[9] https://www.csoonline.com/article/3051123/leadership-management/cybersecurity-spending-more-does-not-necessarily-mean-better.html

[10] https://www.observeit.com/blog/new-ponemon-institute-study-insider-threats-lead-to-big-losses-and-significant-costs/

[11] https://www.observeit.com/blog/why-consistency-in-incident-response-is-important/

One element of earning additional budget is gaining buy-in from stakeholders. According to the EY Global Information Security Survey (GISS)[12], cybersecurity budgets are higher in organizations that do these three things:

1. Place dedicated business line security officers in key lines of business
2. Report at least twice a year on cybersecurity to the board and audit committee
3. Identify non-IT crown jewels and differentially protect such assets

Why are these strategies successful? They help bridge the gap between the security team and the rest of the organization through frequent communication and shared goals, which helps make budget requests about the business as a whole — not just one department.

Making a Case for Additional Budget

Arm yourself with statistics and context: Third-party statistics will help give credibility to your case. Refer to the research in this resource and other sources to prepare for budgeting conversations.

Detail the cost of any past breaches: Perform a cost analysis on the repercussions of prior breaches. Collaborate with other stakeholders, especially finance, to get the data you need.

Approach leadership with proposed budget and time required for training: Detail how budget will be allocated and what resources you need beyond obvious expenditures like technology. The more specific your proposal, the more prepared and well-researched your request will seem.

[12] https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

Final Word

There's a dire need for increased budget around Insider Threat Management, as indicated by the stats and trends around a lack of overall spending in this area relative to need. With 87% of organizations saying they require up to 50% more funding for insider threats, the time is now to take preventative budgetary action before a costly incident takes place.

Being equipped with the right data can help make the case for a stronger insider threat budget. And the right people, processes, and technology can help prevent insider threats from happening within your organization. Even one incident avoided or damage limited can prove invaluable to your organization, and well worth any substantial investment of time, money, and resources.

If you're in the process of evaluating budget for insider threat software, look for a platform that combines user activity monitoring with detailed analytics, so you can gain both visibility and context into employee and third-party contractor activity.

To learn more about ObserveIT's Insider Threat Management platform, which helps with insider threat detection, investigation, response, and prevention, visit our website at observeit.com.

Visit **observeit.com**
to learn more.