observe it

What is Cybersecurity ROI?

Many businesses view security as a pure cost center. They may recognize that certain security investments are necessary, but they may have zero expectations of any return on that investment.

While it's true that money must be spent on people, processes, and technology in order to build a successful security program, security can indeed provide a return on investment. Cybersecurity ROI is real, and businesses who take the time to dig into the numbers may find themselves pleasantly surprised at the results.

Since our focus is on Insider Threat management—and since this is arguably the area of security with the highest potential ROI—today we'll take a look at how programs designed to mitigate Insider Threats can be tracked in order to demonstrate ROI.

Equipped with this information, teams can continue to secure the budgets they need to combat Insider Threats, while also getting a voice and a seat at the table by demonstrating the value of what they do.

observe it

Track Insider Threat Incidents

In order to demonstrate the return on investment in security—and specifically Insider Threat programs—we recommend that teams track Insider Threat incidents. As you may know, the majority of Insider Threats are actually the result of accidents or negligence. This means that many can be stopped with the right combination of training and awareness, so spending money on these areas can bring about quick returns in the form of incident prevention.

To demonstrate ROI, track how incident numbers change over time using Insider Threat metrics. With observation, you should be able to determine which prevention and mitigation tactics work best for your organization and thus where to focus future budget to improve results. Additionally, track the average cost of investigation, containment and remediation for incidents over time (according to research from the Ponemon Institute, these are three of the four most costly areas of Insider Threat management).

Ideally, the business should aim to both reduce the overall number of incidents and to decrease the cost of resolving each incident by catching it early. Insider Threat tools should affect both of these numbers positively, making this an excellent place to identify and maximize return on investment.

observe it

Track Security-Driven Sales

A strong security program with an Insider Threat component can also help drive revenue by demonstrating secure and compliant practices that allow the business to maintain their customer base and win net-new deals.

Your Insider Threat program should include adopting and propagating security and compliance frameworks, such as GDPR, SOC 2 and other industry-specific regulations. Track the number and amount of sales you are able to make that would not be possible without investing in Insider Threat management.

For large businesses and those operating within highly regulated industries, there is often massive upside from a properly implemented Insider Threat program that includes compliance and security efforts. For this reason, customer acquisition is an important area that can quickly and efficiently demonstrate return on Insider Threat program investment.

Compare Reactive and Proactive Costs

Another valuable way to measure and demonstrate the ROI of your Insider Threat program is to track your costs over time in the areas of reactive vs.

proactive efforts. In essence, tracking proactive and reactive costs will allow your business to compare the cost of your preventative efforts to the cost of reactive response and containment efforts.

Proactive Costs	Reactive Costs
Monitoring and Surveillance	Investigation
User Education & Training	Escalation
Security Awareness Programs	Incident Response
Personnel	Remediation
Real-Time Policy Reminders	Ex-Post Analysis

In general, proactive Insider Threat efforts cost significantly less than reactive ones, so demonstrating that you are spending your money on proactive efforts to reduce or altogether avoid surprise reactive costs down the road can also help make the ROI case.

If you're looking for more insight into average Insider Threat costs to ballpark the above or to benchmark yourself against, we recommend checking out these Insider Threat statistics. It can be useful to chart potential costs based on your industry, size, customer base, and other unique factors.

observe it

Earning Back Your Insider Threat Investment

Insider Threat programs hold the potential to decrease the number and cost of incidents, increase sales, and shift the balance from costly reactive measures to cost-effective proactive efforts. As a result, these programs should be viewed as an investment with significant return potential, as long as they are managed properly. In the best-case scenario, an Insider Threat program can be the biggest cybersecurity ROI the business realizes.

By mitigating Insider Threats and cutting the number of security incidents by half, ObserveIT delivers instant ROI.