CASE STUDY

Risk Management Team Uncovers True Cost of Global IP Theft

Problem
The tech company's self-service portal was easy to penetrate by thieves. But was it worth it to plug the security holes? No one could get their arms around the true cost of losses.

Solution
Using RiskLens, the risk management team gathered and analyzed for the first time the likely impact of the IP theft.

Results
With a quantified view of their risk, management could approve an effective security budget.

The Problem

It came up in a casual conversation between risk management team members and an intellectual property manager. He had been wringing his hands for months over the problem but couldn't find a way to convince senior management to take it seriously.

This global technology manufacturing company distributes software updates and other trademarked data to customers via an online portal. But the authentication process to access the portal had a serious flaw: Once in the portal, anyone could download materials to compete with the technology company's authorized partners to service its products.

It was a global threat to the lucrative service contract line of business. At the same time, easy access to the portal was an important feature of the company's commitment to its authorized partners. The IP manager would have to make a strong case if he had any hope of getting management to buy in to an investment in controls. But he couldn't put a number on the losses.

The Solution

Using the RiskLens workshop features, the team set out to quantify the company's risk or, in the terms of the FAIR model, the probable frequency and probable magnitude of future losses.

For the frequency side of the equation, the team worked with the IP manager to compare total downloads from the portal with known authorized downloads to get a fix on probable stolen downloads. Knowing the typical range for number of downloads per customer, they could get an idea of the number of threat actors out there and their download activity.

For the magnitude figure, they could multiply by the value of service contracts for a range of the amount of lost revenue, recognizing that they couldn't fully know how many service contracts the bad guys were fulfilling out of one portal log-in. "The hackers weren't giving us any data," laughs one of the team members.

The risk analysis stuck to potential primary losses. Secondary losses would principally be legal costs to go after thieves around the world, but legal action had been so infrequent, the team didn't think the data was strong enough.

The Results

The results were eye-opening. For the first time, management could see a range of losses, with the understanding that, because the risk team had been cautious about sticking to solid data, the actual impact was certain to be much higher. "Everyone saw the value and the logic of the FAIR analysis," says the team member. "They thought it was pretty cool." The only questions were over the data, which had never been gathered by the company before, and was new to management. The analysis inspired several initiatives in the company to gather more data to feed further analysis, particularly on the legal side. And management approved an ample budget for new controls on access to the portal.

Aggregate Loss Exposure

The aggregation of all independently analyzed risk scenarios.

Maximum	$6.1B
90th %	$2.2B
Most Likely	$104.5M
Average	$962.7M
10th %	$111.7M
Minimum	$2.1M