

BE FREE

CASE STUDY  
BE FREE OF RISK

# Filling the Gaps to Protect Intellectual Property

An engineering firm was concerned that relaxed information security defenses might have paved the way for the leakage of its trade secrets

## Briefing

The engineering firm manufactures industrial mining equipment to shake through ore and help mining operators reclaim waste. After an audit, the executive leadership team noticed a flood of similar mining equipment in the market being offered by competitors. They needed to test the security parameters around IT to see if there was the possibility of trade secret leakage.

TALK WITH OUR EXPERTS [1.877.222.8615](tel:1.877.222.8615)

© Copyright 2014 BestIT.com, Inc.  
All rights reserved.

# Protecting Intellectual Property

## Client

Engineering Firm

## Industry

Mining Equipment

## Challenge

The engineering firm needed to determine if gaps existed in its information security controls at its U.S. headquarters and international offices. Language barriers and differences in international laws made it difficult to perform a thorough assessment of all sites since IT wasn't directly linked to its global headquarters.

## Services Provided

- Vulnerability Assessment
- Internal & External Attack & Penetration
- Wireless Attack Penetration
- Security Roadmap
- Limited Physical Security Check

## Benefits

- Executive insight into gaps in the IT security controls
- A go-forward strategy to patch vulnerabilities and standardize IT policies at all international sites
- Recommendations for a formal IT governance structure and policy overhaul

## Introduction

Theft is a crime that has affected mankind throughout time. Technological advancements have made it easier for thieves not to be physically caught in the act. Now they can steal the intangible. Every year, cybercriminals steal the ideas, inventions and creativity that consistently redefine what it means to be innovative. Intellectual property (IP) theft costs companies \$300 billion each year in the United States alone. It's a problem that spans across the globe.

Our client, a multinational engineering firm, manufactures industrial mining equipment to shake through ore and help mining operators reclaim waste. The intellectual property rights that they hold on their best-in-class mining equipment has allowed them to dominate the marketplace after nearly a century in business. Trade secrets make up two thirds of the value of a business's information portfolio. That amount can be as high as 80% for a knowledge-based industry like manufacturing.<sup>3</sup>

## The Problem

After going through a financial audit, the executive leadership team noticed a flood of similar mining equipment in the market being offered by competitors. The engineering firm has offices throughout Europe and South America with additional locations in South Africa, China, India and Indonesia. Leadership was concerned there might be security gaps within the IT environment not only at the United States headquarters, but also in the offices around the globe. They needed a security assessment to determine if potential gaps in IT security could have led to the theft of intellectual property.

The international business units had a unique set of challenges that would make the security assessment a bit more complicated to execute. Not only were there different outsourcing contracts in effect with local IT firms at each office, there were also numerous language barriers to take into account. Countries also have unique standards for information security and the blueprints for the equipment varied depending on mining laws and equipment standards.

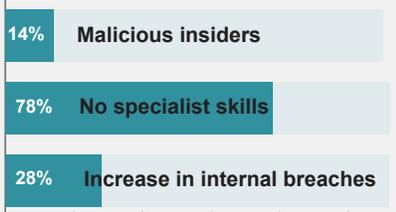
The engineering firm also did not have an IT leader to oversee global IT operations.

## The Solution

After months of interviews, the executive leadership team hired a global IT director

## Quick Look

### Intellectual Property Theft, Corporate Espionage and Hacking



**14%** Malicious insiders account for 14% of all breaches<sup>2</sup>

**78%** In 78% of breaches that occurred in 2013, no special skills or resources were needed to pull off the attack<sup>2</sup>

**28%** Mining companies have seen a 28% increase in internal threats like insider theft in the past year<sup>1</sup>

**U.S. companies lose \$300 billion each year due to IP theft.**

Sources:

<sup>1</sup>EY Global Information Security Survey, 2013

<sup>2</sup>Verizon Data Breach Investigations Report, 2013

<sup>3</sup>Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape, 2013

who was instrumental in coordinating the security assessment at the international sites. The BestIT security team was able to scan the headquarters in three weeks—going through processing systems, wireless security, physical security, policy and procedures and the architecture.

A full assessment of the international sites would not be possible since they weren't connected directly. The solution was to send over a questionnaire with basic questions about what they had and did not have to give the security team an idea of what type of security issues they might have. After a few survey drafts and a workable response rate, BestIT was able to determine what was needed at the international sites to bring security up to par to protect the firm's intellectual property.

### The Results

Based on the scan and survey responses, BestIT concluded there was no overall IT standard or corporate governance for the company. Each business unit had insight into the intellectual property and it was possible to download diagrams, blueprints and other IP and store it locally at each site.

After delivering the 110-page final report outlining all of the vulnerabilities at the U.S. headquarters and international offices, including a list of the top 10 vulnerabilities they should focus on, BestIT recommended that they put a formal governance strategy in place for all of the sites, update the firewall protection and implement security monitoring and intrusion detection to start. BestIT also provided a security roadmap to provide guidance on integrating the new security controls within the existing environment. The international engineering firm is currently working on implementing those recommendations to strengthen its information security controls.

### Conclusion

This engineering company knew that their IP was at risk and called BestIT to conduct a security assessment to determine what needed to be done to protect the business. A security roadmap was laid out for IT regulatory compliance to help protect the intellectual property of the business.

Not all security breaches can be prevented, but there are controls you can put in place to seal the gaps. Contact BestIT today to see how our security services can help you get your security program up-to-date to protect your business investments.



**Contact us for more information.**

BestIT HQ  
3724 N. 3rd Street  
Phoenix, Arizona 85012

+1.877.222.8615 | [info@bestit.com](mailto:info@bestit.com)  
[www.BestIT.com](http://www.BestIT.com)