

"iRAM gives our customers the independent, third-party assurance that their operations and property are protected, and that safeguards are in place to constantly improve physical and network security."

iRAM Client in China

Risk Assessment and Monitoring: An iRAM Case Study

The Challenge

Many companies have global footprints and multiple overseas businesses, which presents a unique set of security challenges. Since most companies lack a thorough knowledge of site-specific (i.e., international) threats and risks, they seek specialists to help them identify and mitigate those risks.

Founded more than 10 years ago, our innovative client is a leader in Internet commerce solutions with millions of users in more than three dozen markets, including the United States and China. The client was concerned that someone might access its global data network from their China facility and how such a breach could affect operations. Since protecting customer data and information is critical to our client's business, they engaged iSIGHT Partners to evaluate their China facility.

The Product

iSIGHT Partners' Risk Assessment and Monitoring (iRAM) service evaluates and protects global enterprises and corporations from human, physical and electronic threats in the United States and abroad. Our iRAM service includes:

- Domestic and international satellite offices
- Global contractors, suppliers and partners
- Offices and intellectual property coveted by fraudsters, including customer lists, passwords, account numbers and personally identifiable information (PII) of employees and customers

The resulting analysis reveals a range of threats mapped to internal vulnerabilities and issues, such as:

- Network policies for access rights to sensitive documents, USB drives and peer-to-peer (P2P) software
- Localized physical and electronic threats, such as in-country hacker groups and organized crime schemes
- Physical and logical vulnerabilities in networks, equipment and facilities

iRAM assessments provide each evaluated asset with a risk score (or "grade"), a list of potential impacts and actionable mitigation recommendations.

The Solution

The iRAM team's unique methods unearthed the client's most likely adversaries and identified key architectural issues and weaknesses in their infrastructure. The iRAM team then provided a comprehensive list of vulnerabilities and actionable recommendations to protect the client from human, physical and electronic threats.

Our customized analysis was derived by combining four separate sources into our assessment:

- **Global audit standards**, such as Control Objectives for Information and related Technology (COBIT) and the International Organization for Standardization (ISO), which allows for a robust examination of security controls surrounding critical assets. In addition, iSIGHT Partners goes above and beyond these standards by benchmarking the methods of leading companies and incorporating their cumulative best practices. iSIGHT Partners can also build custom audits to meet any client's specific needs.
- **Physical walkthroughs** include facility entry points, health and safety issues, "red team" exercises and social engineering tests using in-country resources to deploy global and local expertise.
- **Network analysis** leveraging iSIGHT Partners' global intelligence network; this analysis uncovers specifically crafted tools and techniques from international hacker groups.
- **Intelligence on logical and physical threats** gathered in multiple languages, details geopolitical issues, fraud trends and customer-specific targets.

The iSIGHT Partners' Difference

While our competitors typically assess international clients using only Western tools and methodologies (with the help of translators), iSIGHT Partners uses local sources, tools and tradecraft and relationships to assess sites from the local adversary's perspective. This blended approach provides customers with a better understanding of the threats targeting their assets.

Our assessments are customized around the client's specific critical assets, such as customer data, development code, proprietary algorithms – and the most direct access point(s) to those assets. In addition, we review what access to corporate networks can be achieved through remote connections.

The Bottom Line

Our iRAM analysis helped the client secure its data and facilities in China and alerted them to localized electronic and physical threats against their digital assets. Our team continues to work with the client to implement mitigation techniques to further secure its global business and has since assessed their European facilities.

To better secure your company's most valuable assets and gain peace of mind, let iSIGHT Partners' experienced iRAM team apply its in-country insight and intelligence via our iRAM product. Contact iSIGHT Partners today to find out how our iRAM team can apply its expertise and help secure your organization.

