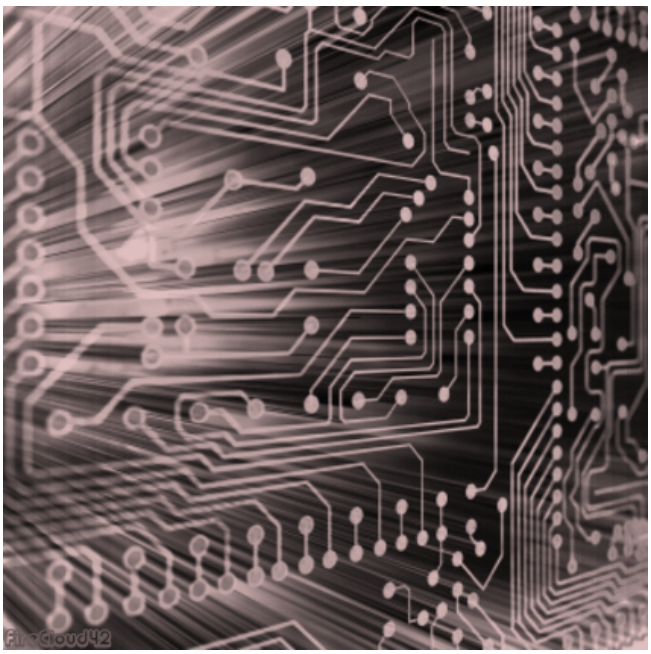

THE INSIDER THREAT TO INTELLECTUAL PROPERTY

BANYAN RISK GROUP | BANYAN RISK GROUP |

Alarm Bells Ringing

The alarm bells started ringing in her head at 11:48 in the morning while performing a routine system maintenance check. The system administrator of a highly restricted series of servers housing her company's proprietary data and intellectual property (IP) detected an unauthorized user in China accessing the servers. These servers contained sensitive product design data and IP for a large international technology company. The administrator challenged the user over instant message with a series of questions regarding his identity and purpose for accessing the servers. The unidentified user claimed he had accessed the servers accidentally, apologized and immediately logged out apparently hoping to elude identification.

The astute system administrator immediately reported this suspicious behavior to her IT Security team. Her timely actions launched a highly complex, international investigation lasting over two months to ferret out the identity of the user, determine what design data he accessed, and understand how he planned to use it.

The investigation was led by the Global Investigations Manager (GIM) who assembled a multi-disciplinary team of experts to identify the unauthorized user, conduct a thorough damage assessment and pinpoint the business processes failures and control gaps exploited by the unauthorized user. After analyzing these findings, the team made and implemented recommendations for improving the security and controls for sensitive product designs and intellectual property on the company's network.

This investigation was conducted and managed by Banyan Risk Group's current Director of Special Projects while working for a large international technology company. He is Banyan Risk Group's subject matter expert on corporate security investigations and due diligence matters.

The Investigation: Hunting the Unauthorized User

The GIM partnered with the company's IT Security Forensic Investigator to determine the identity of the unauthorized user. Close collaboration between the two investigators was essential to ensure the investigation was conducted discreetly, without alerting the unauthorized user that he was under investigation.

The GIM's initial goals were to understand the business processes and controls that governed access to the data, identify the processes and parameters for collaboration using design data between design centers around the globe, and determine the exact data the unauthorized user had accessed on the penetrated servers. The GIM interviewed the system administrator who discovered the unauthorized user and key members of the IT teams responsible for administering the company's network for storing and sharing design data and IP between design centers throughout the U.S., Latin America, Western Europe, Israel, China, and Southeast Asia.

At the same time, the IT Security Forensic Investigator set about doggedly following the unauthorized user's trail through the company network's maze of servers and tools to identify which employee's User ID was used to access the company's servers without the required permissions and to discover the scope of the breach. The IT Security Forensic Investigator determined that the unauthorized user tried to hide his trail by attempting to delete his digital footprints in the network after being detected.

The GIM's inquiry concluded that the company had failed to modernize decades-old protocols that were designed to facilitate easy and open collaboration between design engineers around the world with little

DELETING HIS DIGITAL FOOTPRINT

The unauthorized user took the following measures to try to cover his tracks:

- Deleted local/network data sources and home directory links
- Used spoof structures to hide the local and network data spaces he had created to store copied data
- Deleted data sources he had accessed but had yet not been questioned about
- Deleted history logs of his activities in the company's design data transfer tool

thought given to how they could be exploited by corrupt employees. These antiquated processes failed to keep pace with today's business realities, risks, and potential legal liabilities. Some of the product designs accessed by the unauthorized user were even the proprietary data of other companies for whom the products were being designed and manufactured. The company also failed to consider the need to restrict access to product design data from non-U.S. Persons, which included many of the company's employees residing outside of the U.S. who worked on certain company products that were controlled under the International Traffic in Arms Regulations (ITAR) program.

The IT Security Forensic Investigator next zeroed in on the employee who was evaluated as most likely to be the unauthorized user and remotely interrogated his company computers. She uncovered abundant incriminating evidence which substantiated the suspicions against the suspect. She determined that he had cracked several employees' passwords, logged into their accounts, and used them to access servers to which he did not have his own access. The IT Security Forensic Investigator was then able to determine when he logged into the other employees' work stations posing as them and track his movements in and out of the company's servers and tools as he searched for the product design data he was apparently seeking.

The IT Security Forensic Investigator also determined that the suspect had created several local and network data spaces to receive and store the copied product design data and used spoof structures to hide his activities. She uncovered that the suspect had downloaded in excess of one terabyte of the company's design data and copied it to five external storage devices. Finally, she also discovered that he had used the company's proprietary tool to transmit some product

IT SYSTEM VULNERABILITIES

The company had failed to modernize decades-old protocols… to keep pace with today's business realities, risks, and potential legal liabilities.

Some of the product designs accessed by the unauthorized user were even the proprietary data of other companies for whom the products were being designed and manufactured.

design data outside of the company to several servers which were located in China, but whose ownership was not discernible.

With the incriminating evidence amassed by the IT Security Forensic Investigator, the GIM next enlisted the assistance of the Vice President in charge of the design center in China and several senior Chinese managers to discreetly corroborate the evidence. Successfully working with the Chinese managers required adroit political maneuvering because they had a tendency to try to shield themselves from the fallout if one of their employees was under investigation or found guilty of stealing proprietary information. Even allowing for the Chinese management team's self-interested protective attitude toward a "star performing engineer", the results of their analysis showed less than 10% of the designs the suspect accessed were related to the work he was doing for the company. The Chinese management team could offer no explanation for his behavior and had little alternative but to fully cooperate in the investigation.

At the insistence of the GIM, the employee was suspended immediately, pending the outcome of the investigation, and escorted out of the design center without being allowed to remove anything from his work area. All of his access to the company's networks and systems was immediately revoked. However, local IT personnel neglected to cut off his Virtual Private Network access and his manager failed to confiscate his company identification badge when he left the building.

Several days after his suspension, the Chinese security manager for the design center reported that the suspect's management team inexplicably had allowed him to return to the design center to participate in an important meeting. The suspect was allowed to move about the design center unescorted, despite his suspension. He was observed in his former work area removing external

NAVIGATING CULTURAL SENSITIVITIES

Successfully working with the Chinese managers required adroit political maneuvering because they had a tendency to try to shield themselves from the fallout if one of their employees was under investigation or found guilty of stealing proprietary information.

storage devices in an attempt to take them with him when he left design center. The external storage devices were confiscated, and the Chinese management team was censured for their lapse in judgement.

Digging himself into a deeper hole, several days later, the suspect was detected accessing the company's Virtual Private Network from home in an additional effort to destroy evidence during the Chinese New Year holiday, when only a skeleton crew of IT personnel were at work.

Exploring Litigation: The Challenge of a Foreign Legal System

Based on the overwhelming incriminating evidence that had been amassed against the suspect, the Legal Department decided to have him interviewed by outside counsel, a Chinese attorney with expertise in IP and Chinese patent laws. The GIM drafted the lengthy confrontational interview script the Chinese attorney would use to conduct the interview.

The confrontational interview lasted several hours, and the interview script produced the intended result: the methodical dismantling of the suspect's denial of wrong doing. The suspect initially denied each of the allegations made against him. After each denial, he was presented with documentary evidence uncovered by the GIM and the IT Security Forensic Investigator proving that he had in fact done everything he was accused of doing. After being confronted with the evidence, the suspect reluctantly acknowledged that he had lied and then admitted to having committed each infraction. However, to the very end, the employee steadfastly denied sending the company's design data to servers in

CHINESE LEGAL SYSTEM CHALLENGES

Major hurdles to intellectual property rights enforcement in China include:

- Local judicial protectionism
- Challenges obtaining evidence
- Exceedingly difficult burden of proof requirements
- Small damage awards
- Perceived bias against foreign firms

China which were outside of the company's network, despite documentary evidence showing that he had done so. The culprit was terminated on the spot.

Based on the GIM's recommendation, the Legal Department sought to file criminal charges against the culprit for the theft of its IP including over three hundred product designs. However, IP protection laws in China are structured so tightly and require such a high burden of proof to show that the victimized company was materially damaged by the theft, that prosecution of the culprit proved to be impossible.

The Damage Assessment: Potentially Catastrophic Consequences

Urged by the GIM's counsel, senior members of the company's product development teams, senior members from several engineering design teams, and attorneys from the Office of the General Counsel were enlisted to conduct a damage assessment of the culprit's activities. They reviewed all of the design data the culprit had accessed and copied onto external storage devices. The team performed its work operating on the assumption that all of the design data had been transferred to servers outside of the company's network in China and were therefore outside of the company's control.

DAMAGE ASSESSMENT CONCLUSIONS

- The company's market leader status for several key products could be significantly damaged if its product design data was provided to its competitors.
- Dual-use technology, including some that was ITAR-controlled, was included in a small number of the product designs that were copied by the employee, though no evidence existed that ITAR-controlled product design data was provided to unauthorized users outside of the company.
- Proprietary design data for products manufactured for several customers was contained in a relatively small number of the product designs copied by the employee, though no evidence existed that the proprietary product design data was provided to anyone outside of the company.

Identifying Exploited Process Gaps: Too Little, Too Late?

In an effort to prevent another large-scale theft of its product design data in the future, the company stood up the IP Protection Committee, a cross-functional committee chaired by the General Counsel to identify the process and control gaps that the culprit exploited. The team consisted of the GIM and representatives from IT Security, Corporate Audit, Legal, the Chief Technology Officer, and key engineering design teams from each of the company's business units.

The team identified business process and control gaps in two categories. Those which passively facilitated the culprit's theft of design data due to being woefully out of date, obsolete, or simply non-existent. And those processes and controls that existed, and were industry standard, but were simply not robust enough to prevent the theft of data by the culprit.

A common theme which permeated both categories of process and control gaps and IT security control failures was an unwillingness to allocate enough funding to add new IT Security controls, tools, monitoring capability, and manpower that would prevent thefts of product design data from occurring. Another and more deleterious commonality uncovered by the IP Protection Committee was the lack of foresight and ability of key decision-makers to accurately assess the risk and consider implementing safeguards to thwart the threat of IP theft by its own employees, in other words they had neglected to consider the classic insider threat.

The IP Protection Committee discovered fundamental flaws in the way the company had split its IT functions into two separate organizations, both with inadequate IT security functions. One IT organization was responsible

LEADERSHIP FAILURES

Did not adequately safeguard intellectual property from insider threats.

Unwilling to allocate enough funding to add new IT Security controls, tools, monitoring capability, and manpower that would prevent thefts of product design data from occurring.

for the company's Linux-based network containing design data and IP while another was responsible for the PC-based network for the rest of the company. The second organization was charged with protecting the company's network from being penetrated or hacked and possessed a standard, but outdated and inadequate, suite of IT Security tools but had no oversight or responsibility for the company's crown jewels - its product design data and IP - which were under the control of the first organization.

IP Protection Committee Recommendations: Thwarting Future Catastrophic Losses

At the conclusion of its deliberations, the IP Protection Committee authorized several key initiatives that the company would implement over the coming months to prevent another catastrophic theft of its IP.

- The IP Protection Committee determined that both IT organizations would be immediately merged into one IT organization to bring the company's product design data and IP under the same level of IT Security and protection as the PC-based systems used by the rest of the company.
- All future product designs created by design engineering teams would be assigned to a single owner within each of the various design teams. The owner would be responsible for determining the need to grant access to engineers from other design teams to the product design data created by his own design team.
- All new designs containing ITAR-controlled and Customer Proprietary product design information would be registered on a new automated tool

Owning the intellectual property is like owning land: you need to keep investing in it again and again to get a payoff; you can't simply sit back and collect rent.

- Esther Dyson, leading technology angel investor, philanthropist, journalist

managed by the Legal Department. All access to these two categories of product design data would have to be formally requested and approved prior to access being granted. This system would ensure better protection of such restricted information and would retain the names and User ID information for all persons who were granted access to these categories of product designs.

- A new enterprise-wide tool would be purchased which funneled all access to IP, product design information and all sharing of product design information through a single portal on the company's network. The new tool would make accessing and sharing of design information easier to control, limit, and track.
- Additional state-of-the-art IT Security tools would be purchased and employed to greatly enhance the ability to detect if product design information and IP were being copied to storage devices connected to engineering work stations and laptops. It would also allow IT Security to detect the exact specifications for all devices, including external storage devices, that were connected to company workstations and laptops, and exactly what information was copied to any external storage device.
- System administrators responsible for maintaining the company's proprietary tool utilized by product design engineers to download and/or transfer massive design data files would be assigned responsibility for monitoring all usage of the tool to identify design engineers who were downloading or transferring product design data that exceeded "normal" usage patterns.

The future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property.

- Richard Posner, Judge on the U.S. Court of Appeals for the Seventh Circuit, in Rockwell Graphic Systems, Inc. v. DEV Industries, 925 F.2d 174 (1991).

Banyan Risk Group Can Help Your Company Protect Its Intellectual Property and Proprietary Information

- If your company has intellectual property, sensitive or proprietary information which is not adequately protected with state-of-the-art IT Security capabilities, Banyan Risk Group can help you assess the data loss risk and legal risk to your company and assist you in designing and implementing robust intellectual property protection systems.

- If your company has inadequate business processes and control gaps creating vulnerabilities to its most sensitive information, Banyan Risk Group can conduct a risk assessment and design a better regimen of business processes and procedures and close control gaps reducing your company's vulnerabilities to theft of intellectual property and proprietary information.

- If you suspect your company's intellectual property or proprietary information has been stolen by an employee or contractor, Banyan Risk Group can conduct an investigation to identify the thief, assess the damage, and recommend measures to prevent future thefts.

- Banyan Risk Group's experts have provided these services and others to effectively safeguard intellectual property and proprietary information to many large international companies and clients.

To review Banyan Risk Group's suite of client services and read some of our past success stories, please visit our website: www.banyanriskgroup.com

---