Crown Jewels on the Network: A Benchmark Study of Leading Companies' Discovery and Protection of Intellectual Property

Naomi R. Fine
President
Pro-Tec Data
Telephone: 650-493-0555
E-mail: nfine@pro-tecdata.com

October 2006

I. Executive Summary

A benchmark study of Reconnex (See www.reconnex.net) customers asked information security professionals in leading pharmaceutical, technology, and software services organizations to describe their: 1) intellectual property protection priorities; 2) requirements for addressing those priorities; and 3) the role that content monitoring and filtering technologies play in meeting those requirements.

The benchmark study participants use Reconnex content monitoring and filtering software to enable the discovery and protection of their intellectual property (IP). The technology allows the companies to locate sensitive information—even in its derivative and amorphous forms—at rest and in motion. These companies learn from what is discovered and monitored, and, based on their learning, determine and implement the appropriate legal, policy, personnel, procedural and technology protections for their intellectual property.

The protection of clearly defined IP, such as patented technologies, requires that all components and derivations of this content can be discovered and monitored on the network. Similarly, the protection of amorphous IP, such as new drug research or new software development, also requires a technology that can locate and monitor such information by key words and phrases, as well as by language (e.g. English text versus C+ source code) and circumstances (e.g. the who, what, where, when, and how of the information activity). Unlike structured data, such as Social Security numbers, the discovery and protection of intellectual property requires a more sophisticated conceptual mapping.

Each participant in our study uses the Reconnex content monitoring and filtering technology because it:

- gives companies the flexibility to protect unique content by defining concept maps and honing those maps as companies learn the words, phrases, languages, and circumstances that define their IP and its risk scenarios; and
- captures a historical archive that allows companies to investigate security concerns by examining past network activity.

Some of the companies in our study, however, had to address internal pushback because of the capture and archive feature, based on privacy and related political concerns.

In addition to providing an important intellectual property protection tool, both in discovering IP on networks as well as monitoring IP leaving networks, companies are also using content monitoring and filtering technology for other purposes, such as searching for evidence of wrongdoing after a company is alerted to suspicious activity. When an employee left to join a competitor, for example, one of the companies in the benchmark study used the capture database to determine whether the employee transferred IP, and to whom, before that employee's departure.

II. Introduction

Hundreds of billions of dollars of intellectual property is birthed, developed, socialized, and brought to its full value using information technology on company networks. A benchmark study of Reconnex's content monitoring and filtering technology users (See www.reconnex.net) reveals how the technology is being used to protect intellectual property in its emergent, developing, and fully developed manifestations. Information security leaders in the participating companies described the intellectual property they seek to protect, their company's intellectual property protection priorities, the value they derive from content monitoring and filtering technology, as well as their concerns and their wish list for further development of the technology.

The companies interviewed represent the pharmaceutical, technology, and software services industries. All company participants were global market leaders.

III. Benchmark Results

A. Pharmaceutical Company

Company Background

The pharmaceutical company is very diverse with 120 facilities in 100 countries. The company has research scientists around the globe and, without content monitoring and filtering technology, the Information Security (IS) organization has no way of knowing where the company's IP is created or where it is transmitted.

Intellectual Property (IP)

The pharmaceutical company is most concerned with protecting its scientific research, including animal testing and drug formulations; strategic business information, such as business plans, competitive analysis, and merger and acquisition data; and manufacturing data, such as batch records and cookbooks. In some cases, less sensitive IP such as network and building diagrams are also protection priorities.

IP Protection Priorities

The pharmaceutical company's priority is to protect the business value of its IP. Achieving this objective requires understanding where its IP is, where it goes, and where it has gone.

Addressing IP Protection Priorities with Content Monitoring and Filtering

The pharmaceutical company uses content monitoring and filtering (as well as digital rights management) to protect IP content in motion and at rest. Content monitoring and filtering technology also provides the pharmaceutical company with an investigating tool. The full capture

feature of the Reconnex content monitoring and filtering technology allows the pharmaceutical company to generate forensic evidence suitable for court proceedings.

A third level IP protection priority is compliance with the Sarbanes-Oxley Act as well as privacy regulations.

Requirements of Content Monitoring and Filtering Technology
Much of the information that comprises the pharmaceutical company's IP is not structured. To protect it, the company needs a means to discover and monitor each instance of its valuable confidential information. The content monitoring technology must help the company define, discover, and monitor amorphous IP.

The corporate IS group serves the company's numerous businesses, many of which want tools to monitor and protect information. One requirement of content monitoring and filtering technology is that it allows managers and other appropriate personnel to manage their data protection directly. Another requirement is the ability to monitor content at the file level.

Solution and Results from Content Monitoring and Filtering Technology
The pharmaceutical company uses content monitoring and filtering technology as a tool to aid with investigating IP leakage. The IS group works within a security organization that has many former FBI agents who are responsible for investigations and responding to security-related incidents. The quality and completeness of the historical data provided by the content monitoring and filtering technology is critical to the legal admissibility of the evidence from their investigations in court proceedings.

The IS group places control of the monitoring and filtering technology in the hands of appropriate users. These users are responsible for balancing the business' interests in determining how and when to control content.

A search may result in hundreds of millions of documents. The user determines when to find information:

- at rest;
- in motion; and
- in the capture database.

The pharmaceutical company finds that content monitoring results provide an effective awareness tool. Users of information technology, as well as those responsible for protecting information, can view, in detailed and summary form, the location and transmission of sensitive company information. In one case, employees set up an internal website and were surprised to see that several users sent the information outside the company's network.

The pharmaceutical company also uses content monitoring as a research tool to discover where the company's IP is located and to help determine where content protection technologies are needed or require adjusting. For example, the Reconnex product's discover feature allowed the company to track down content which, by policy, could be disseminated externally but only if encrypted.

Over time, the pharmaceutical company expects that the content monitoring tool will help it identify users' behavior and information usage patterns that can be used to further refine the concepts to be discovered, monitored, and searched. The IS group also expects to craft and refine its protection policies based on actual practices discovered as a result of content monitoring.

Concerns and Internal Pushback
The pharmaceutical company had concerns about the capture database created by the Reconnex solution, and received internal pushback on privacy grounds regarding its use. The pharmaceutical company found this to be an issue particularly in European countries, such as France, England and Italy, which have stricter privacy standards than the United States and must meet EMEA requirements. The company addressed these concerns by restricting access to the capture database only to those people involved with investigations, taking into account country-specific privacy standards.

B. Technology Company

Company Background
A large portion of the technology company's multi-billion dollar profits are derived from licensing royalties on patents and other IP. With several hundred licensees around the globe, the company is continuously handing off its IP in the form of know-how and prized material goods. There is a group at the technology company dedicated to licensing, monitoring, and enforcing the use of the company's patents globally. The technology company has 60 offices around the world, including India, China, and the United Kingdom.

Intellectual Property
The technology company is most concerned with protecting its core technology. Even a summary description of it might reveal the technology company's identity; therefore, it is not included in this report.

IP Protection Priorities
The technology company's priority is to ensure that its IP is protected from the moment it is conceived through the patent filing process, delivery to licensees, and marketplace use.

A major challenge is that the technology company was founded by former professors who believe that an open, academic-like systems environment fosters innovation and creativity.

Addressing IP Protection Priorities with Content Monitoring and Filtering
The technology company uses content monitoring and filtering technology to support each component of its intellectual property protection strategy:

1) Legal mechanisms: include patents, licensing, and litigation. Content monitoring locates innovation sensitive content so that it can be protected where it resides, and also ensures that licensed IP goes only to licensees. The captured data in the historical archive provides a forensics tool for litigation.
2) Process-based controls: include checks and balances to ensure that the right licenses are in place. Content monitoring and filtering prevents IP documentation from being released until configuration management, release engineering, business process analysts, and customer care groups confirm that everything is in place for the release.
3) Technological controls: include information security strategy. Content monitoring and filtering aids policy development, forensics, and intrusion detection by discovering IP at rest, monitoring IP in motion, and allowing the analysis of historical network activity.
4) Accounting and auditing: includes policy compliance. Content monitoring and filtering provides an audit tool to ensure policy compliance.
5) Education and awareness: includes user understanding of risks and responsibilities. Content monitoring gives users a snapshot of risks and reinforces their responsibilities to protect sensitive information and IP.

Requirements of Content Monitoring and Filtering Technology
The technology company's primary requirement for content monitoring and filtering is that it must provide a system that prevents information leaks and protects IP rights from inception of the information to patent filing, delivery to licensees, and beyond.

To meet the technology company's requirements, the content monitoring solution had to:
1) include robust fingerprinting technologies with key word, key phrase, and concept matching;
2) apply concept-based filtering technologies; and
3) scale across the global enterprise, while being tactically managed from corporate headquarters in the United States.

Solution and Results from Content Monitoring and Filtering Technology
The technology company uses content monitoring to detect leakage of its valuable IP. The company focuses on high priority areas, such as the transmission of a document that has been identified as proprietary or confidential to a competitor via internal or Internet-based email.

The technology company finds that a lot of intelligence must be used to build rules to refine the filtering system. It uses context to determine if there might be a data leak, which avoids false positives.

The technology company also uses the data captured from content monitoring for security investigations and forensics.

Content monitoring is transparent to users as deployed by the technology company. Although passive monitoring and detection is the current approach used, the company's ultimate goal is to employ enforcement capabilities to actively control data leakage.

Concerns and Internal Pushback
Information Security (IS) reported no pushback on using content monitoring and filtering technology. Rather, IS was asked: "Why aren't you doing more?" This reaction comes from those who benefit from the capabilities of the content monitoring technology. When IS reports that someone is FTPing source code to an employee's home computer, for example, IS is given accolades for tracking the incident. Management and HR appreciate the results of content monitoring because they are able to work with the individual involved in FTPing the source code to create a different process for working on the source code from remote locations (if appropriate). As a result, the technology company reduces its information security risk should the employee's relationship with the company be terminated

C. Software Services Company

Company Background
The software services company must protect not only its own IP, but also all the IP and other sensitive information entrusted to it by its customers. Many of the company's customers evaluate the software company's security before purchasing its services.

Intellectual Property
Initially, the software company's primary concern was with protecting its lead generation information from leaving the company and going to competitors and business partners. As the company has matured, it has focused on protecting any sensitive information that might affect the company's reputation as well as product road maps, business deals, credit card and other non-public personally identifiable information.

IP Protection Priorities
The software company's priority is to protect information which, if unprotected, could damage the company's competitive advantage, its reputation, or its relationships with customers. Such information is often amorphous and frequently unknown until it is leaked or some type of security compromise is suspected.

Meeting IP Protection Priorities with Content Monitoring and Filtering
The software company uses content monitoring and filtering technology to support each component of its IP protection strategy:

1. Personnel: includes education and awareness raising and reinforcing employees' responsibilities to protect sensitive information. All employees are told that the company uses content monitoring software.
2. Process: includes vetting information releases through legal, public relations (PR) or human resources (HR) departments. Monitoring allows the company to determine if information has been disseminated before it is approved for release. Based on a historical review of the content monitoring archive, legal, PR, and HR representatives can determine if sensitive information (or some part or variation of it) was disseminated, without authorization, to customers, partners and others. Similarly, when an employee's performance is being evaluated, or when an employee is subject to a performance improvement plan, legal or HR can request a historical lookup of that employee's network activity. In this way, it can be determined if the employee leaked sensitive company information by sending it to an e-mail account, a partner, a competitor, or some other unauthorized recipient.
3. Policy: includes setting an expectation of privacy. The company notifies employees that their network activity is monitored, which limits employees' expectations of privacy.
4. Technology: includes using access controls and firewalls. The content monitoring and filtering technology assists IS in determining where technology controls are needed or should be improved.

Requirements of Content Monitoring and Filtering Technology

The software company's priority is to use a content monitoring and filtering technology that does not require identifying sensitive information up front. Many of the software company's employees and users do not label documents properly, and it would be too burdensome to require users to register information as sensitive. In many cases, it is only after the fact that someone working for the company realizes that information developed, received, or transmitted, is sensitive.

Historical searching after information is identified (or suspected) as sensitive, and monitoring information flow over time, is also a high priority for the software company. The software company needs to see what information is going where, and what information has gone where, to determine what, if any, remediation is needed.

Another priority for the software company is using content monitoring to conduct internal risk assessments. The software company audits for IP fingerprints in email, images, and instant messaging, to ensure that the content monitoring system is alerting security personnel to actual policy breaches rather than triggering false positives.

Solution and Results from Content Monitoring and Filtering Technology

Prior to deploying the content monitoring technology, an employee from the sales group sent a scathing email to the CEO of the software company's competitor. The CEO of the competitor forwarded the email to the CEO of the software company. It took two software company employees two full days to determine who sent the original scathing email. The software company estimates

that with the content monitoring technology now in place, this exercise would take one person about an hour, rather than taking two people two days.

During a risk assessment, the software company discovered that an employee was communicating with outsiders to plot connecting the company's network to an underground network that would allow malware agents to be downloaded from the Internet to the software company's network. The content monitoring technology enabled the software company to prevent this disaster from happening.

The software company's risk assessment also provided insights into the dissemination of its lead generation information. Based on these insights, the company was able to improve its processes for discovering, monitoring, and protecting its lead generation information.

Content monitoring provides the software company with a window into what is being done on its network and, when a suspicious activity is discovered, to search for past activity and corroborating evidence. The company uses content monitoring to:

- monitor for security breaches in real time; and
- search the capture database to find, in minutes instead of days, the perpetrators of security breaches.

Concerns and Internal Pushback

Many in the software company were concerned that the capture of all content traversing the network provided some in the company, and particularly those in IS, with access to highly sensitive information, including the contents of executives' emails. This is viewed by IS as a political, rather than a privacy concern. The IS group addressed these concerns by limiting access to executives' email to two security team members who are prohibited from reviewing executive information unless the company's General Counsel is involved.

The software company's executives are requesting that content monitoring be used to monitor and report on employee productivity based on the employee's network traffic. Executives want to know how some employees are spending their time. Are they visiting customer web sites, as they are supposed to, or are they sending personal emails?

While the software company has not yet embraced such use of content monitoring technology, it is not far from it. For example, the company uses content monitoring to determine who is seeking jobs via competitors' web sites.

IV. Summary and Key Takeaways

Content monitoring and filtering technology is an IP protection tool. It allows companies to locate the roots of IP—sensitive data and information—and implement legal, policy, personnel, process, and technology protections to safeguard it.

Protecting IP requires a sophisticated solution that can recognize sensitive content in all of its variants and amorphous forms. For example, sensitive product development information may include a conceptual description of a new product, functional specifications, cost and budget analysis, performance studies, test results, proposed development schedules, and product availability dates. This content can only be discovered and monitored on a network if the content monitoring technology can recognize it in its unstructured, variable, and derivative forms.

To be useful, the content monitoring solution must incorporate complex intelligence to distinguish circumstances that represent risk from those that do not. Monitoring technology can only distinguish between a proposed product budget sent to a competitor and a proposed vacation budget sent to an employee's spouse at that same competitor if the solution incorporates the idea of concepts into its IP detection mechanisms.

IP concepts provide a means to define – and therefore detect, monitor, and control – unique content, in all its permutations. The ability to monitor by context, such as who sent what where, when, and how, and using content variations to account for the amorphous nature of IP, ensures a company's IP is intelligently protected. Likewise, the ability to search an archive and explore the historical context of an incident adds to the depth and value of the protection.

The benchmark participants in our study use the Reconnex solution, in part, because it allows them to define IP concepts that take into account not only key words and phrases, but also context—who sent what to whom, when, and how. For example, sensitive information related to new drug development may be discovered and monitored as some combination of:

- key words, phrases, or codes;
- senders and/or recipients; and
- communication channels.

In developing IP concepts, the benchmark participants in our study use an adaptive feedback loop:

- The company defines its IP, including typical and derivative representations.
- The monitoring technology scans the network, including servers, email gateways and user machines, to discover IP at rest and the circumstances of its use and transmission over the network.
- The company uses the results of the discover process to develop IP fingerprinting concepts, which incorporate the circumstances of IP use and transmission and distinguish sensitive from non-sensitive information and authorized from unauthorized transactions.

- The technology monitors for IP content using multi-vector, concept-based detection, and alerts the company to rule violations.
- The company investigates rule violations by searching the capture database, which allows the company to understand the historical circumstances of the security incident.
- The company refines IP detection mechanisms to incorporate lessons learned and eliminate false positives. As a result, the company continuously enhances the accuracy and effectiveness of the content monitoring technology.

As is clear from the process described above, the benchmark participants rely on the capture database feature of the monitoring technology to investigate security incidents. For example, after receiving an alert that an engineer used file transfer protocol (FTP) to transfer the company's source code to a server on another company's network, IS used the capture database to review all of the employee's FTP activity and all of the employee's correspondence with the company to which he sent the source code.

The capture database also allows these companies to investigate security events that are triggered offline. When an employee announces that she is leaving the company to work for a competitor, for example, the company can use the capture database to review all of the employee's recent network activity and specifically her correspondence with her future employer.

The benefits of the captured information are not without cost. Participants in our study indicated that there are privacy and related political concerns that arise from capturing a record of the content traversing the company's network and maintaining sophisticated tools that allow such content to be mined. The technology solution to this concern is to provide a feature that allows companies to limit data capture and its access.

In addition to providing an important IP protection tool, companies see other benefits from content monitoring and filtering technology. For participants in our study, the technology is also:

- an investigation tool for security incidents;
- an awareness tool for employees and management;
- a prioritization tool for IT security; and
- a productivity tool for HR management.

Content monitoring and filtering technology is a relatively new technology. As it matures and more companies use it, the benefits and concerns will certainly evolve.

About the Author

Naomi Fine, Esq., President and CEO of Pro-Tec Data, founded the firm in 1985 to help companies manage and protect confidential information and intellectual property. Ms. Fine is a nationally recognized authority whose depth of knowledge comes from working with hundreds of world-class companies to identify sensitive information, assess needs for protecting it, develop tailored strategies, establish policies and procedures, and provide training and tools that secure competitive advantage. Ms. Fine has been cited by Fortune, Business Week, Time, USA Today, the New York Times Cybertimes, the Los Angeles Times and The Industry Standard as a leading expert in her field. Ms. Fine's work for Apple Computer, MCI, and Tandem Computers has been described as exemplary in industry trade journals, including The Personnel Journal, Sales & Marketing Management, and Security Management. Ms. Fine is an authoritative and enthusiastic speaker for many industry associations, as well as being a published author of numerous articles related to information and intellectual property protection. Prior to founding Pro-Tec Data, Ms. Fine was a business attorney counseling high technology companies on protection, licensing and other transactions related to intellectual property. Ms. Fine can be reached at nfine@pro-tecdata.com.

