

## Intellectual Property Rules

**Date:** February, 2007

**Author:** Eric Ogren, Security Analyst

**Abstract:** The Four Rules of Intellectual Property Leakage Protection serve as guidelines for security teams deploying technology to protect their businesses against information loss. Security teams are acting to more quickly discover sources of intellectual property, providing comprehensive protection against leakage of IP. Security technology exists to assist security teams in automating protection processes while offering better protection against the major threats to IP leakage.

### The Four Rules for Intellectual Property Leakage Protection

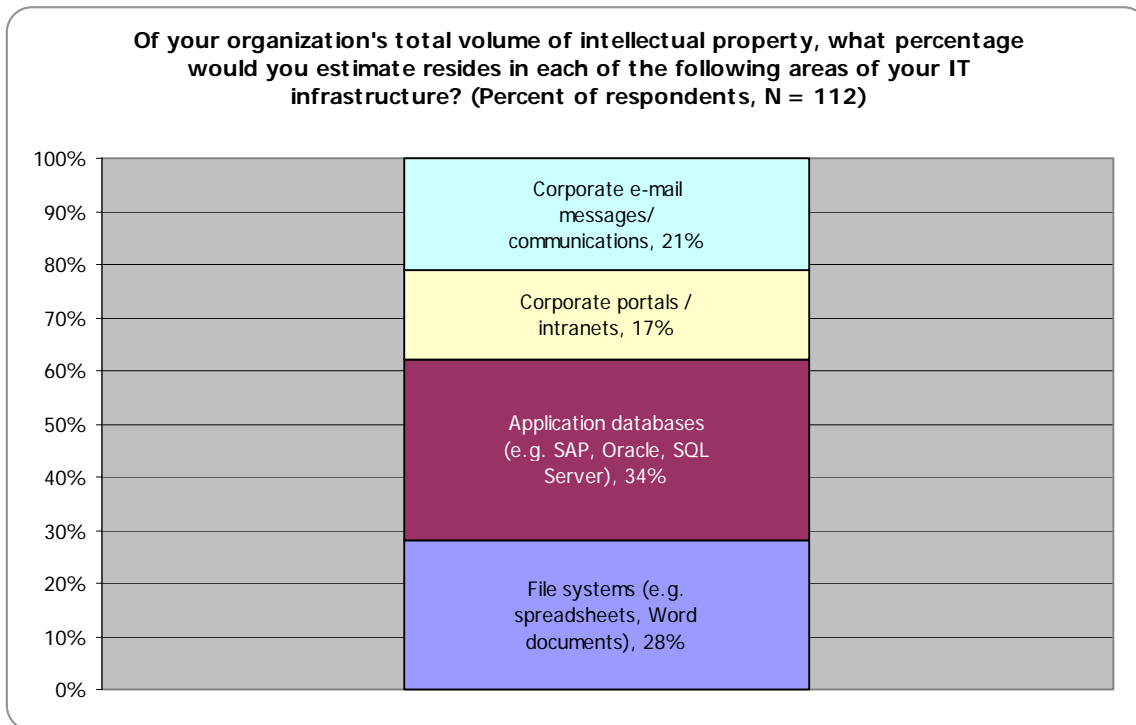
Enterprise IT is charged with securing electronic forms of intellectual property against leakage and inappropriate use. Traditionally, the initial focus had been on “personally identifiable information” (PII), where disclosure-oriented regulations have gained the attention of enterprise boardrooms around the world. However, PII is just one special instance of the larger challenges faced by corporate leadership while protecting against the leakage of intellectual property. Security and IT officers require comprehensive solutions to protect the business against unauthorized leakage of all electronic forms of IP.

In 2007, protection of intellectual property is a high priority for most organizations. According to primary research conducted on behalf of Reconnex, 90% of the organizations surveyed will deploy new technologies to secure electronic forms of intellectual property within the next 12 months. The requirements of an enterprise-wide IP protection solution must satisfy basic rules:

- **Rule #1: Electronic copies of IP appear in many forms.** The simplest forms of information to recognize are those that contain the fixed formats of credit card numbers, social security numbers or the existence of keywords such as “confidential” or “proprietary”. However, IP also includes forms that are much harder to recognize, such as financial information, customer contracts and agreements, product development specifications and other types of trade secrets. Solutions for protecting the organization against IP leakage need to have the flexibility to allow organizations to customize definitions of IP and significant intelligence to identify intellectual property as it moves in the network.
- **Rule #2: Intellectual Property appears everywhere in the network.** The organization’s IP is widely distributed throughout the corporate network, not only transmitted in e-mail messages but also residing as documents in file systems, tables in application databases and objects in Web portals (see Figure One). Security products must be flexible in identifying formats of IP - a search for fixed format credit card numbers only scratches the surface. The broad distribution of IP calls for a strategic solution that remains aligned with the requirements defined by the various lines of business.

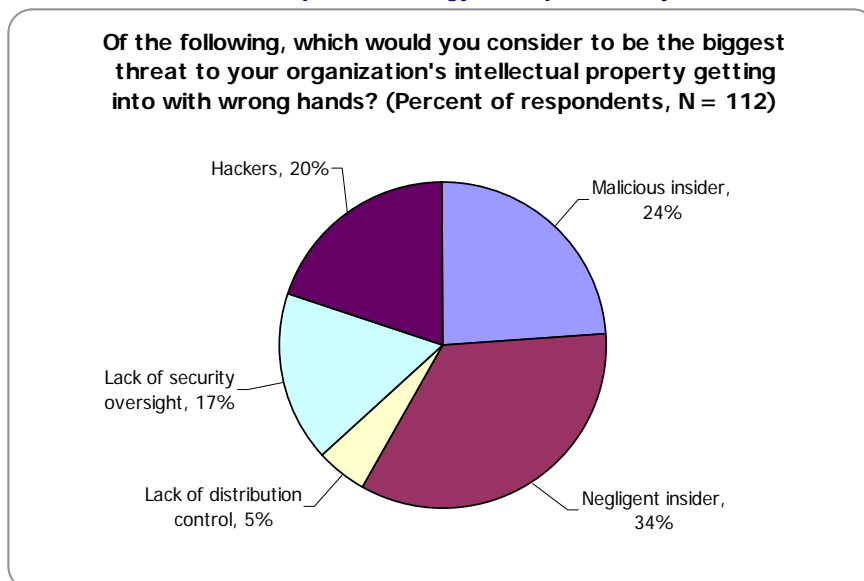
The leading repositories for IP are databases and unstructured file systems, with e-mail and Web portals comprising only a part of the requirements. Endpoint software solutions would need to be installed wherever IP resides to provide security oversight, which ESG considers to be an impractical approach. Network appliance solutions have the visibility into the various sources of IP and can present a consistent IP leakage management interface to the organization.

**Figure One: Source of Intellectual Property**  
*Source: Enterprise Strategy Group, January 2007*



- Rule #3: Insider misuse is a large threat to the business.** Organizations trust their employees, contractors and outsourced staff to operate in the best interests of the enterprise. However, ESG research indicates that 58% of respondents believe that malicious and negligent users represent the biggest threat to an organization's intellectual property getting into the wrong hands (see Figure Two). While still a very real security concern, outside hackers represent a lower risk for the loss of IP. ESG believes that the insider threat to the leakage of intellectual property will retain its high risk rank, as organizations increasingly outsource privileged administrative functions.

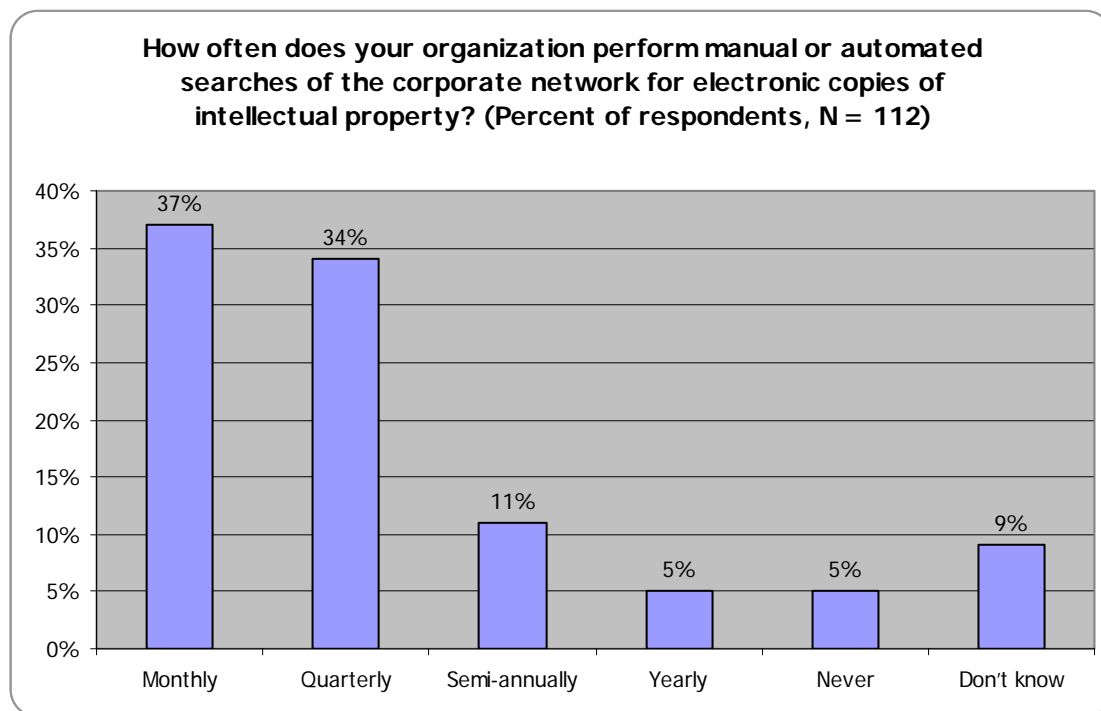
**Figure Two: Insiders are the Largest Threat to IP Leakage**  
*Source: Enterprise Strategy Group, January, 2007*



ESG believes that protecting against the leakage of all electronic forms of intellectual property requires the independent oversight of corporate security teams. IT operations should be focused on delivering IP through business applications to knowledge workers. However, the independent auditing and detection of IP leakage requires the operational controls of a security system. Research results show that the leakage of intellectual property and personally identifiable information is most often detected either by security systems or from inside the organization (65%).

- **Rule #4: Comprehensive programs to protect against IP leakage can require extensive resources.** Protecting against the leakage of IP is a continual process, requiring frequent searches of the network to discover electronic copies of IP and compliance with corporate security policies (see Figure Three). IP is constantly being created in databases, file systems, e-mail communications and Web portals across the enterprise. Manual procedures used to discover new electronic copies of IP are both costly and error-prone. ESG believes corporations that started with PII-specific programs are now broadening their requirements to optimize resources consumed in discovery and audit activities.

**Figure Three: Intellectual Property Protection Requires Automation**  
*Source: Enterprise Strategy Group, January, 2007*



The main purpose of network appliance-based technology is to automate the discovery of IP in a network. This procedure not only saves money by avoiding manual procedures, but also tightens security by reducing the window of time that IP exists without the protection of corporate security. ESG believes that the automated discovery and classification of intellectual property is a critical requirement for organizations deploying IP leakage protection systems.

### Practical Steps

Security technology is ready to be deployed in order to help IT administration secure electronic copies of intellectual property.

ESG recommends the following practical steps for organizations investing in IP security:

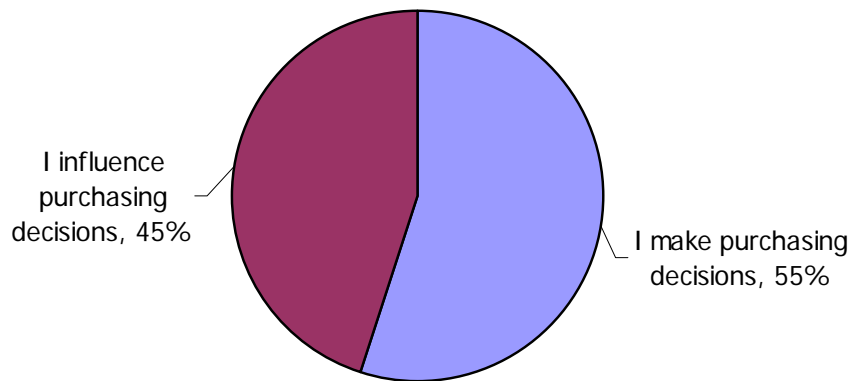
- **Define comprehensive requirements for IP and PII at the same time.** Personally identifiable information is a form of IP for most organizations, with the main difference being the procedures an organization must take to abide by disclosure regulations. Definitions of IP change at the rate of business. Protecting against IP leakage also protects against PII leakage.
- **Segregate IP protection duties.** Research shows that approximately 58% of IP leakage is traced directly to insider actions, with only 20% of IP leakage attributable to malicious outsiders. It pays to mimic the best practices of audit firms by empowering security teams to provide independent oversight of operations.
- **Automate discovery of intellectual property.** Organizations spend a great amount of time and money searching the network for electronic copies of intellectual property. In fact, 71% of organizations surveyed perform this task at least once every quarter. Companies deploy intelligence tools that can recognize the many forms of IP in networked resources such as file shares, databases, e-mail and Web portals. Discovery is a critical step in managing IP controls.
- **Evaluate network-based solutions.** ESG research shows that 90% of respondents expect to purchase technology within the next 12 months with the hope of reducing the risk of IP leakage. Network-based approaches can discover IP and detect leakage without the administrative overhead of distributed software.

### The Bottom Line

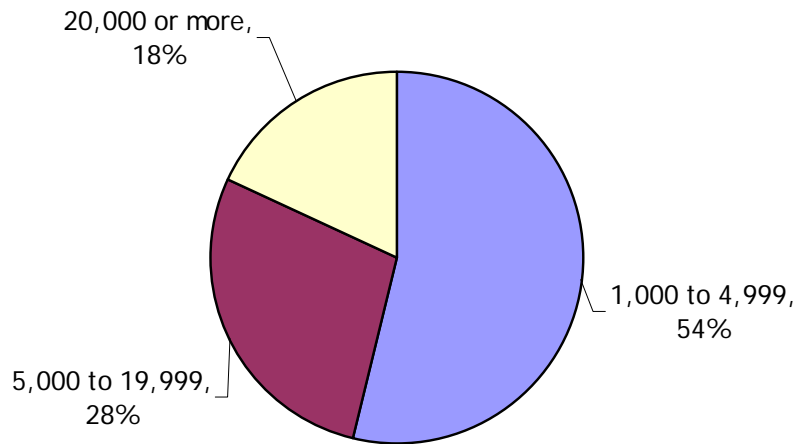
Security officer agendas are dominated with activities assuring that the enterprise is compliant with government regulations and is protected against the loss of intellectual property. This can be a daunting task as intellectual property, which includes personally identifiable information, permeates the network in databases, file stores, e-mail repositories and Web portals. The Four Rules of Intellectual Property Leakage Protection guide security teams deploying technology to protect the business against information loss. Reconnex offers non-invasive network-based technology that, when used properly, can help organizations deploy IP leakage protection that meets the requirements of the Four Rules of IPLP. ESG recommends that enterprises follow the Practical Steps in evaluating solutions to protect Intellectual Property.

**Securing Intellectual Property  
Primary Research Results**

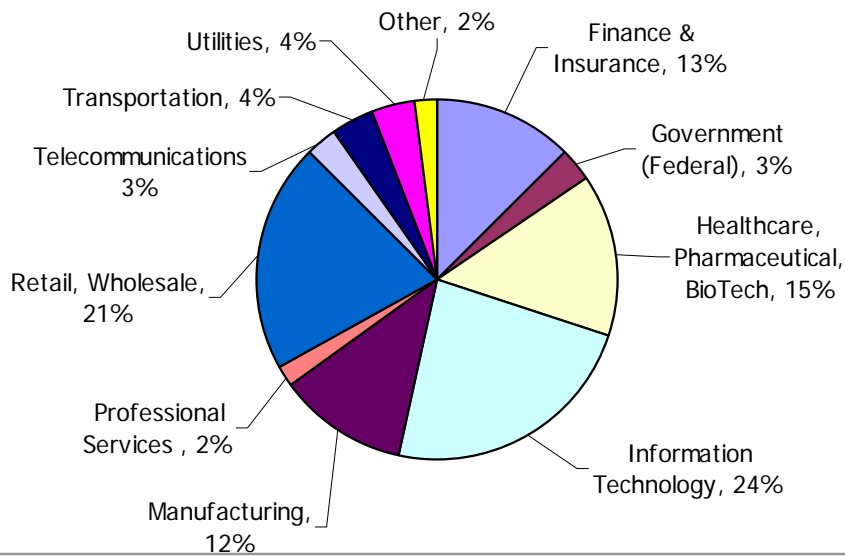
**Based on the previous definition, please describe your role in your organization's purchasing process for solutions that secure electronic forms of intellectual property. (Percent of respondents, N = 112)**



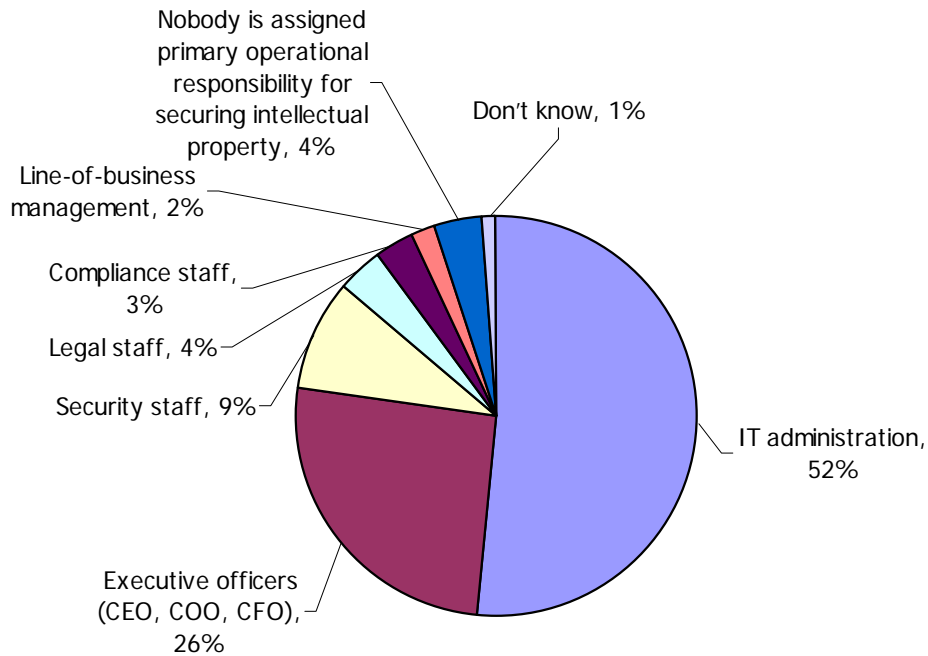
**How many employees does your organization have worldwide? (Percent of respondents, N = 112)**



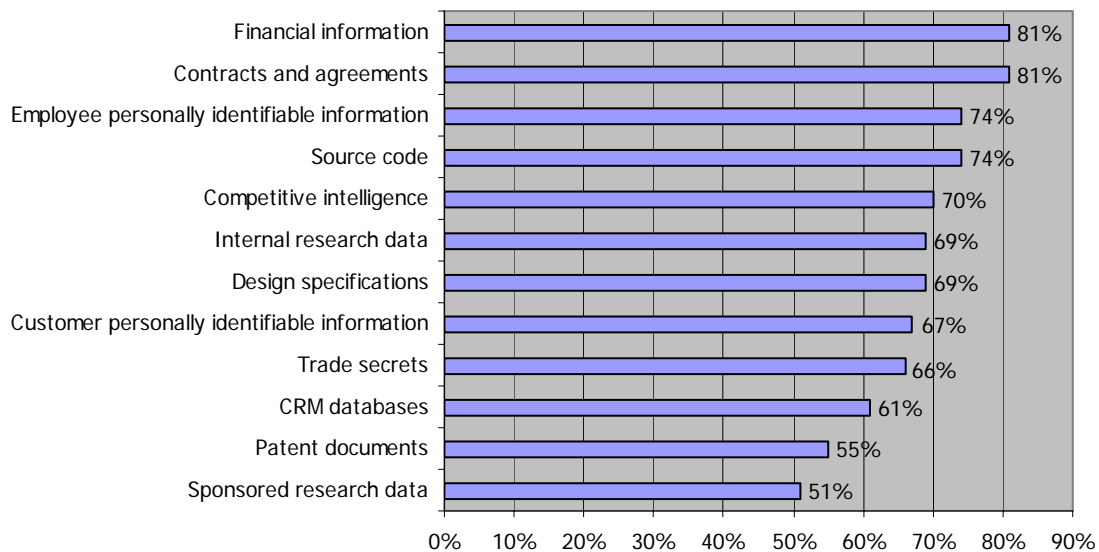
**Which vertical industry best describes your organization? (Percent of respondents, N = 112)**



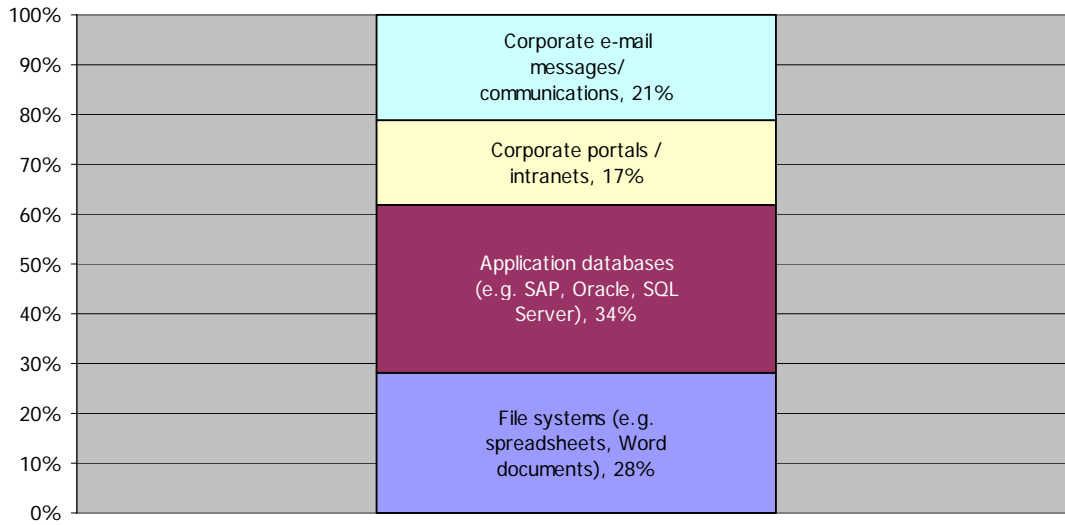
**In your organization, where does primary operational responsibility (as opposed to legal or fiduciary responsibility) for securing electronic copies of intellectual property reside? (Percent of respondents, N = 112)**



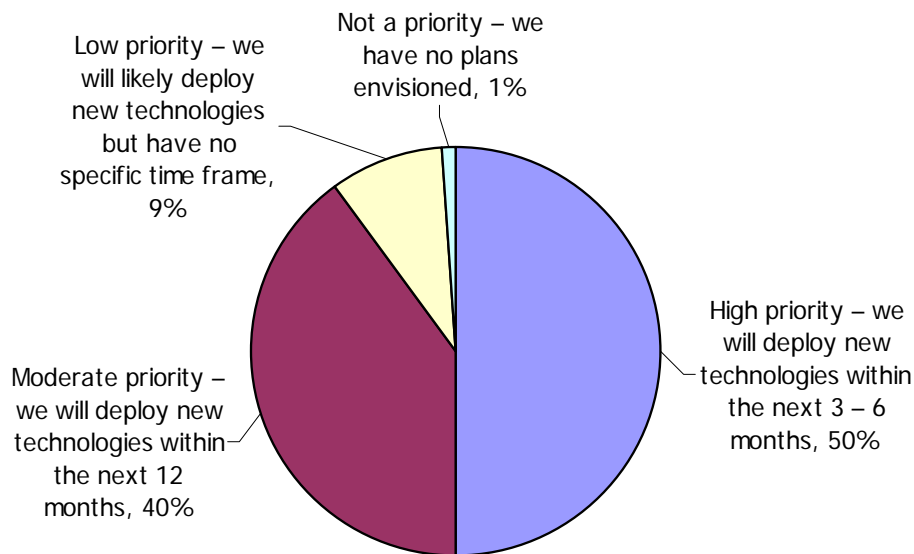
**Which of the following elements would you consider to be part of your company's intellectual property? (Percent of respondents, N = 112, multiple responses accepted)**



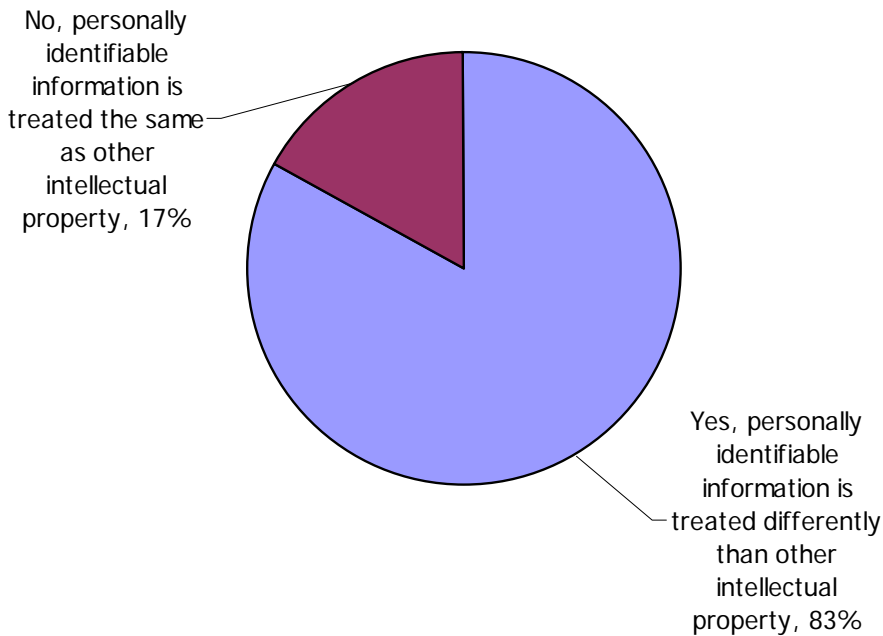
**Of your organization's total volume of intellectual property, what percentage would you estimate resides in each of the following areas of your IT infrastructure? (Percent of respondents, N = 112)**



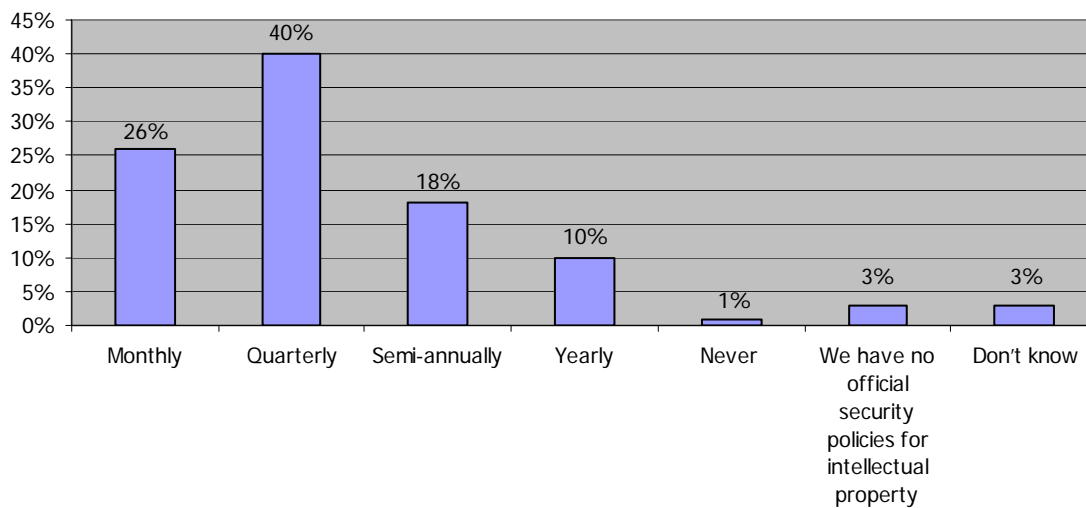
**What priority would you say your organization has assigned to deploying new technologies to secure electronic copies of intellectual property? (Percent of respondents, N = 112)**



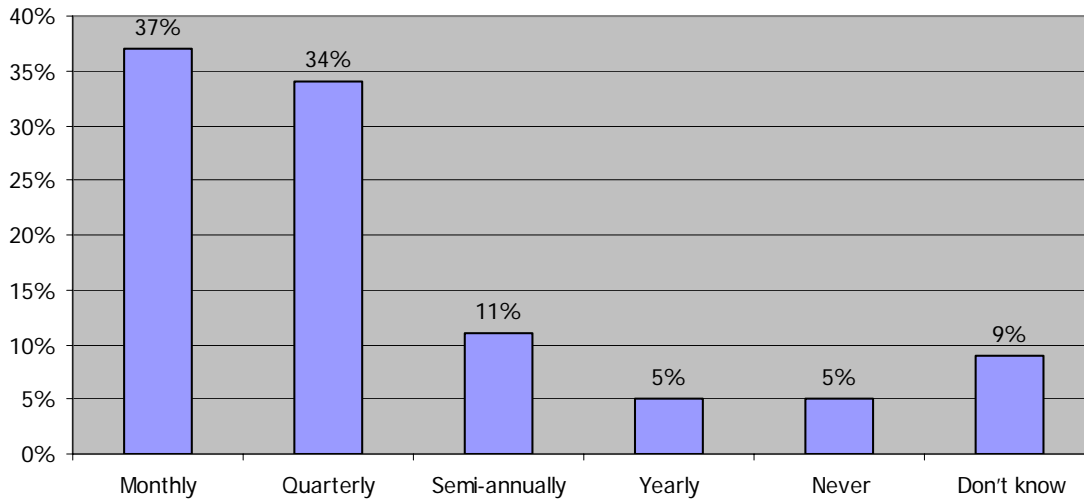
**In your organization, do policies for securing personally identifiable information differ from policies for securing other forms of intellectual property? (Percent of respondents, N = 112)**



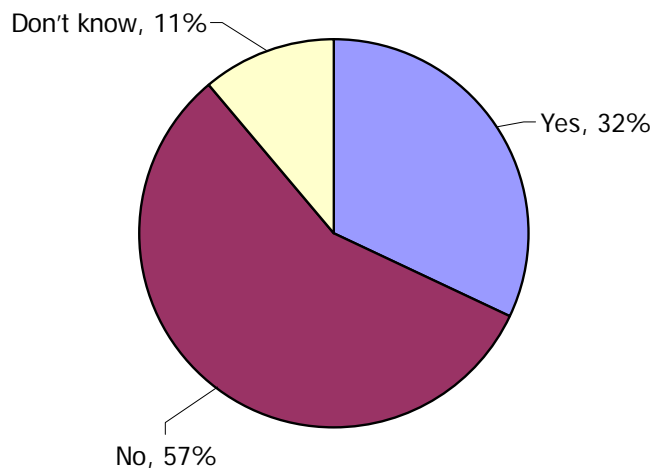
**How often does your organization review its security policies for intellectual property? (Percent of respondents, N = 112)**



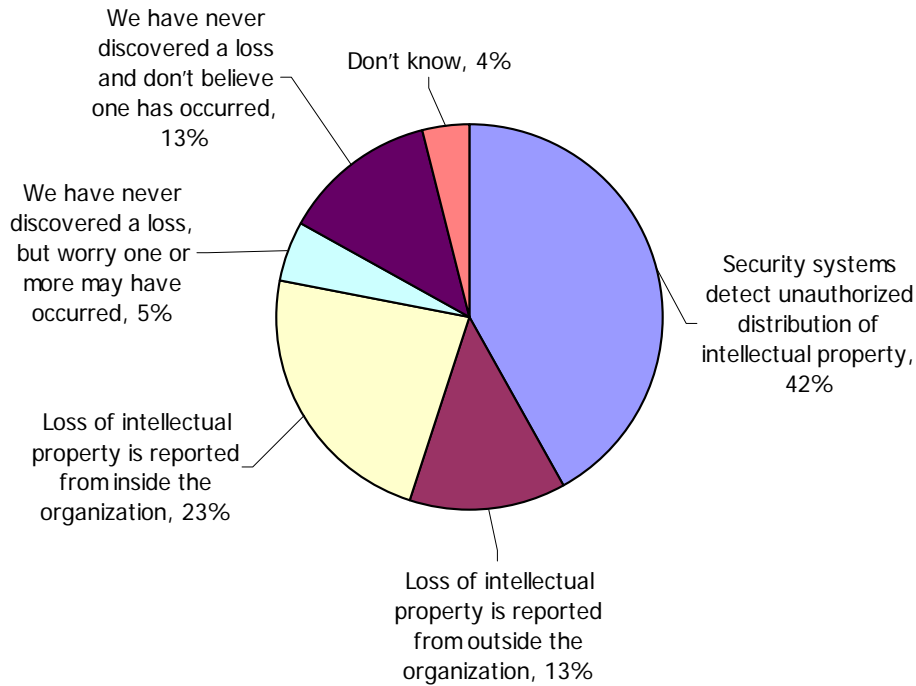
**How often does your organization perform manual or automated searches of the corporate network for electronic copies of intellectual property? (Percent of respondents, N = 112)**



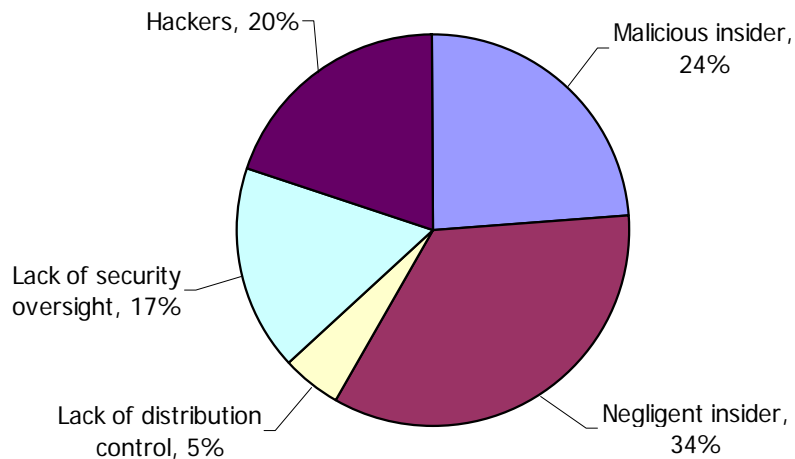
**Has your organization experienced a loss of electronic intellectual property within the past 12 months? (Percent of respondents, N = 112)**



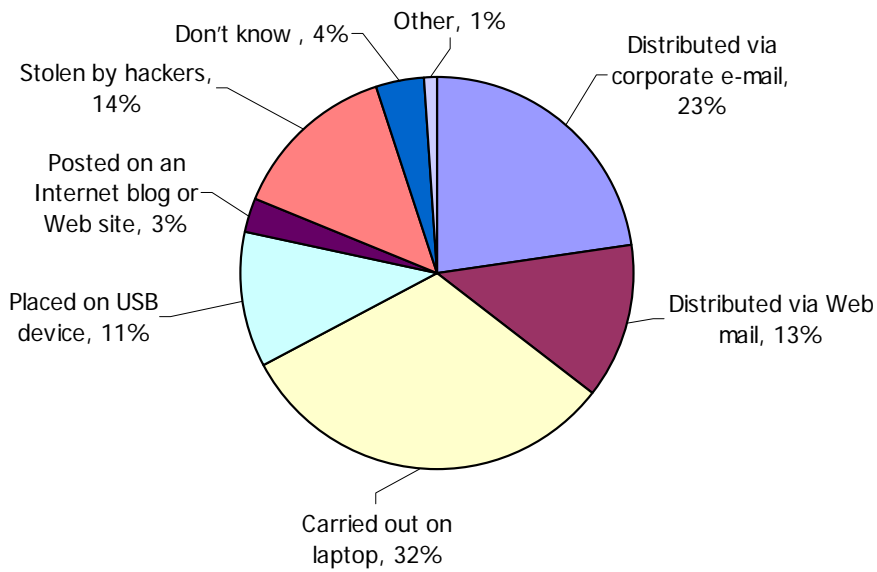
**In general, how is your organization most likely to discover the loss of electronic intellectual property? (Percent of respondents, N = 112)**



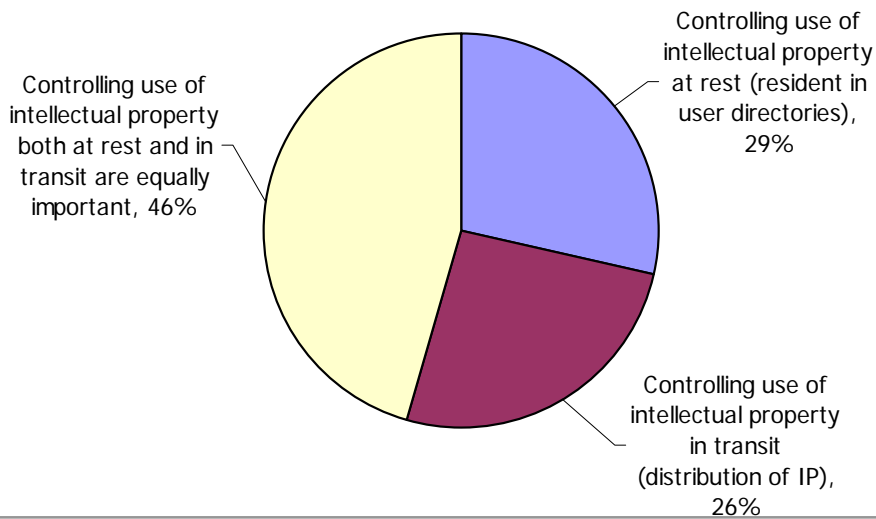
**Of the following, which would you consider to be the biggest threat to your organization's intellectual property getting into with wrong hands? (Percent of respondents, N = 112)**



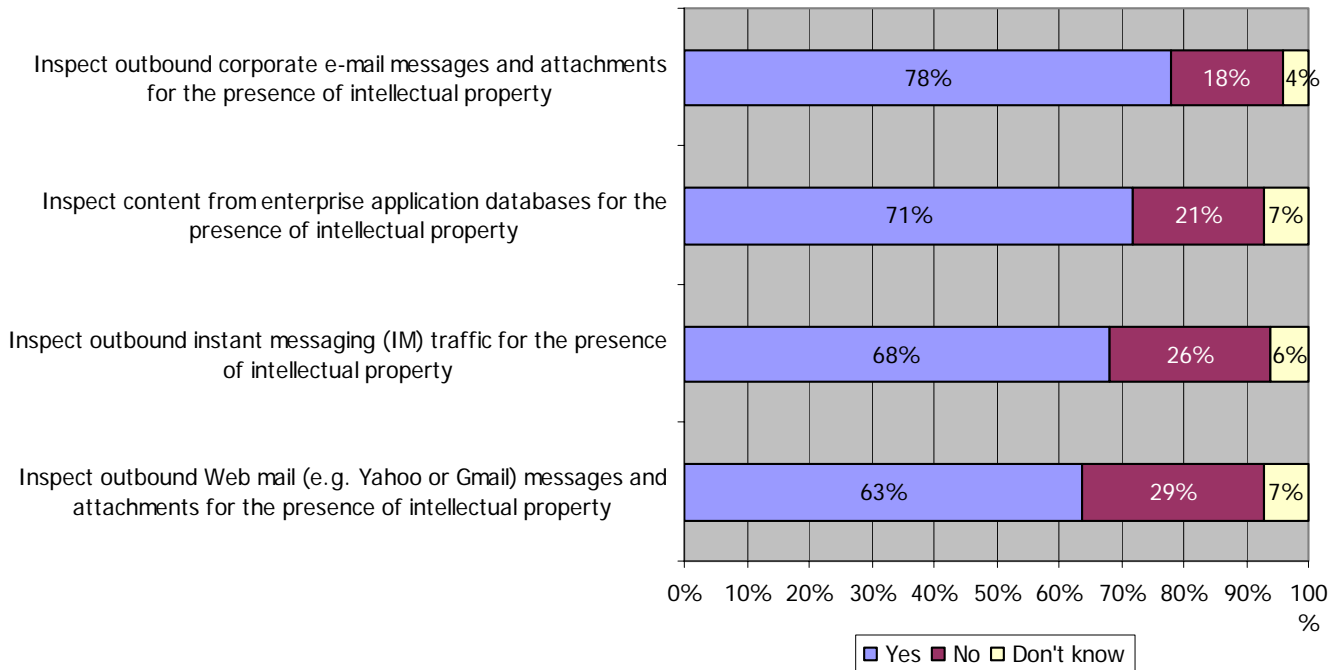
**Of the following, how is intellectual property most likely to leak out of your organization? (Percent of respondents, N = 112)**



**Which of the following would you say is the most important aspect of securing the use of intellectual property in your organization? (Percent of respondents, N = 112)**



**Please indicate if your organization currently employs any of the following processes. (Percent of respondents, N = 112)**



All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.