

# Insider Threat

# I3P

Institute for Information  
Infrastructure Protection

## A Critical Challenge

Difficult to detect and prevent, attacks by people with legitimate access to an organization's computers and networks represent a growing problem in our digital world. These insider threats frustrate employers who lack the resources to identify them and monitor their behavior.

Insiders are not just employees: today they can include contractors, business partners, auditors... even an alumnus with a valid email address. And not all insider attacks are malicious; the perpetrators may be unknowing pawns of a malevolent colleague or a poorly-tested system, or simply the careless initiator of unintended consequences. But one thing is clear: insider threats are a costly problem, bedeviling organizations that lack the resources to monitor actions, prevent bad outcomes, or avoid harm when data leakages occur.

The underlying complexities of insider threat, including the very definition of an insider, are poorly understood. At the same time, protective and mitigative strategies are difficult to implement without impairing normal business operations. The Institute for Information Infrastructure Protection (I3P) *Insider Threat* project brings a grounded, multidisciplinary and far-reaching approach to this critical cyber risk. The project will have a significant effect, not only on how employers view insider risk, but on how organizations can effectively respond to potential threats and actual behaviors. The technologies and policies developed by the project team will balance business needs with effective security solutions.

## Project Overview

Supported by the I3P, the *Insider Threat* project brings together more than 20 experts from seven major institutions and numerous fields of study to unravel the myriad complexities posed by insider threat.

The project has two clear objectives:

- To gain in-depth understanding not only of the types of insiders but also the range of threats they pose. To achieve this goal, team members are conducting a comprehensive study of malicious behavior, from motivation and intent to response strategies and likely consequences.
- To develop tools and processes that will protect critical infrastructures against insider attack, with an emphasis on demonstrable results. As the work progresses, team members will make prototype technologies available for demonstration and testing by corporate and government partners.

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded laboratories, and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States.



The prospect that not all insiders are trustworthy raises several pertinent questions. For example, what factors cause an insider to act inappropriately? What incentives will encourage an employee to stay on the straight and narrow? And what are the appropriate responses to negative insider behaviors?

## Working with Industry

*Insider Threat* researchers are actively working with industry and government stakeholders to elicit feedback, amass data and experiences, and test new technologies. This partnership will ensure that solutions are comprehensive and useful, aligning good security with real-world needs.

Focused on deliverables, the team is leveraging its relationships with industry, most notably in the financial sector, to test tool prototypes early in the development cycle. The team also seeks partnerships with vendors to facilitate the marketing and distribution of tested technologies.

## Team Members

Dartmouth College  
Columbia University  
Cornell University  
Indiana University  
MITRE Corporation  
Purdue University  
RAND Corporation

## Making an Impact

Tools that alert companies to possible unwelcome insider actions already exist. They track and monitor patterns of network activity, looking for signs of unusual behavior, such as repeated attempts to access a generally restricted site. But such systems can be burdensome and sometimes produce false positives. They can also overwhelm a large network by slowing traffic and interfering with business operations. And since insiders have legitimate access, security controls can be circumvented by employees with the right constellation of privileges and technical skills.

The *Insider Threat* project acknowledges that security must complement, not hamper, business needs. To that end, team members are compiling a comprehensive overview of insider behavior, describing the roles of motive, intent and policy in enabling wrongful actions. In addition, researchers are identifying risk factors for each type of insider behavior, plus methods and incentives to discourage inappropriate activities. Moreover, unlike most other technology-based endeavors, the I3P's *Insider Threat* project incorporates legal, economic, ethical and technical concerns in its suite of detection, mitigation and prevention solutions.

Specific goals of the *Insider Threat* project include:

- Bringing clarity and context to the definition of the insider, including the categorization and identification of different kinds of insider actions and motivations
- Devising a taxonomy of insider threat that includes access policy, motivation and intent
- Developing tools in collaboration with industry so that I3P technologies are compatible with real-world needs
- Incorporating ethical, legal and privacy concerns into strategies for combating insider threat
- Analyzing schemes for access assignment, so that excess authorization and privileges are revoked when not needed
- Developing detection strategies that can distinguish harmful from benign behavior, including the use of honey tokens for studying aberrant behavior
- Building threat models from actual data derived from experiments with real insiders
- Creating a monitoring and filtering system that works well, even on large networks, to assess behavior and prevent data leakage
- Evaluating the business impact of mitigation methods, including behavioral incentives and deterrents
- Producing a framework for risk management that includes the valuation of assets to be protected and the organization's perception of risk
- Gaining insights that will inform training programs, raise awareness among employers, and perhaps reshape the way employees think about their actions

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



Institute for Information  
Infrastructure Protection



“People think of cyber security as an electronic fortress that repels hackers and criminals bent on breaking into computer systems from the outside. But cyber security does little to repel inside attackers, those with legitimate access to a company’s computers. How does one know, for example, if the system administrator acted wrongfully? Finding ways to safeguard networks against inappropriate insider behavior—whether malicious or benign—is a national security imperative.”

Shari Lawrence Pfleeger  
RAND Corporation  
and Team Leader

Information about the project  
can be found at

[www.thei3p.org](http://www.thei3p.org)

or by contacting  
Shari Lawrence Pfleeger,  
Team Leader at  
[pfleeger@rand.org](mailto:pfleeger@rand.org) or  
Charles C. Palmer,  
I3P Director for Research at  
[charles.c.palmer@dartmouth.edu](mailto:charles.c.palmer@dartmouth.edu)

The I3P is managed by Dartmouth College

