IMPERVA®

An Inside Track on Insider Threats

"You can't take it with you."

But many people do, that is, when it comes to corporate data.

To stem the problem, companies have resorted to technology. But this is only part of the solution. Successfully mitigating insider threats requires security teams to play psychologist, implementing a broader effort that reminds employees of their moral obligations. This means involving the human resources and legal departments, as well as working with business units, to create an environment that reminds employees that data and intellectual property (IP) do, in fact, belong to the enterprise. Technology helps reinforce, audit, and validate good behavior.

Insider Threat Defined

A trusted person who has access to intellectual property or data, and who uses that information outside of acceptable business requirements.

Misuse of information may be due to malicious intent, an accident, or compromise by outsiders.

One of the key hurdles security teams face is altering employee perceptions about data and IP ownership. Startling attitudes about data were revealed in a 2010 street survey of 1,000 Londoners, from entry level to executive level. 70 percent of the people surveyed planned to take something with them when they left their current job: 27 percent plan to take intellectual property, and 17 percent plan to take customer data. Most telling: A majority of the employees surveyed felt that they own the data, and therefore felt justified in taking it.

The same survey indicates that these attitudes are not being addressed by employers. 79 percent of the respondents stated that their organization either does not have data removal policies for employee departure, or they were unaware of such a policy. Furthermore, 85 percent of employees store corporate data on their home computers or personal mobile devices.

These ordinary citizens represent a serious hazard to security: The **insider threat**.

The insider threat is not just a phenomenon of Western culture—it's a problem for any society that has digitized its business processes and stores sensitive data or intellectual property. The exact same survey, conducted in Shanghai and Beijing, revealed that while only 36 percent now feel they own their data, 62 percent had taken data when they left a job in the past; 56 percent admitted to internal hacking, and 70 percent admitted to accessing information they should not have.

These surveys indicate that the temptation to access or procure company property, including data, is cross-cultural and part of human nature.

While hacking gets more attention from the media and many security professionals, insider threats can have a larger impact. Perhaps the very reason that the problem is so under managed by businesses and their security teams is that it is so pervasive and overwhelming, every employee is a potential threat.

Existing research on insider threats reflects the industry's uncertainty in dealing with the problem. Many solid studies and surveys nicely describe and quantify the problem. Most recently, a Carnegie Mellon study recently found that "Roughly half of all companies record an insider incident; about three-quarters do not report the event to law enforcement; and firms typically split over whether their insider attacks are more damaging than their external compromises."[1] Another study from FTI Consulting found that, on average, it takes financial service firms almost 32 months for victim organizations to detect fraud coming from insiders.[2]

Today, however, it is difficult to find a set of current and common practices for mitigating the risk of insider threats.

A New Approach: The Imperva Common Practices Study

To provide a starting point for companies to address the insider threat head-on, Imperva conducted its own study to reveal effective practices in a variety of organizations. Our objective was to create a catalog of effective real-world practices to be used as a benchmark and a source of ideas for organizations embarking on this process. And yes, we are a vendor. However, our results do not emphasize products and technologies. Rather, our research highlights the importance of nontechnical aspects, such as the role of human resources and legal to greatly influence the moral dimension of an enterprise.

Methodology

Our study loosely followed the model used in the book ***Good to Great*** by Jim Collins. Collins started with a list of 1,435 companies, examined stock market performance over a several year period, and identified 11 that outperformed their peers. Collins' team then studied the 11 in depth to identify the characteristics of "great" companies and their leaders.

Doing the same in security is very difficult. Public information on breaches is hard to procure, making true benchmarking very difficult. However, Imperva started with a sample of 1,000 companies, and identified the top 40 that have successfully managed and prevented insider threats. We interviewed many firms, narrowing our pool based on:

- Strong need to internally protect data or intellectual property.
- A security team with more than four years of experience with insider threats.
- Low number of breach incidence resulting from an insider threats in the past two years.

[1] http://www.darkreading.com/insider-threat/167801100/security/security-management/240007900/watch-the-watchers-trusted-employees-can-do-damage.html
[2] http://www.sei.cmu.edu/reports/12sr004.pdf

The companies that qualified for our study were diverse and global:

- Geographies represented included the USA, Australia, Europe, South America, and South Africa.
- Industries included banking, insurance, government organizations, agriculture, medical device retailers, computer equipment manufacturers, entertainment companies, and online platform developers.
- Revenues ranged from a few million to billions.

Because we were looking for companies that are innovating and breaking new ground to protect against insider threats, our study was designed to catalog what is working, regardless of how common or uncommon a practice may be. We sought out the techniques that forward-thinking companies use now, and a majority of companies will use in the future. Therefore, the output of our study is a qualitative list of effective practices, rather than an exhaustive, quantitative, statistical approach. However, when we saw a practice recur in more than 50 percent of the firms we examined, we called it out.

The practices we uncovered fit into four categories that parallel the process that our target companies followed in implementing their security strategies:

- Establishing Business Partnerships
- Prioritizing Initiatives
- Controlling Access
- Implementing Technology

These practices are common "best practices," but only best for the companies that use them. We don't anticipate that a "one size fits all" methodology will emerge from our findings. Our objective in creating this catalog is to let companies 'cherry pick' the practices that are right for them.

"Insider Threat" Defined

With our interviewees, we agreed upon a common definition of "insider threat":

A trusted person with access to intellectual property or data who uses their privilege in excess of acceptable business requirements or practices.

Misuse of information may be due to:

- Malicious intent
- An accident
- Or, being a compromised insider, usually via malware

It is worth noting that many organizations focus on malicious and accidental breaches, and not on breaches caused when employees are the victims of outsider hacking, malware, and the like. Insiders who leave themselves open to being compromised are a growing source of the insider threat.

Part #1: Establishing Business Partnerships

Typical businesses view InfoSec (Information Security) as a policy cop, paranoid custodian, and overall barrier to progress and innovation. A February 2012 Forrester report, *Navigate the Future of the Security Organization*, summarized the issue with great clarity: "They see people in the IS profession as technologists, not equals. The No. 1 complaint from the board is that they are stuck dealing with very complex and technical people."

Typical InfoSec teams are failing to demonstrate a return on security investment (ROSI), or—even to outline how their day-to-day activities protect the intellectual property—valued data assets, and even reputation of the business. As a result, business units—even other parts of IT—frequently bypass InfoSec until the end of a project, and then order them to "make it secure."

The atypical companies in our study find innovative ways to partner with their internal customers and earn their seat at the table. The practices in this section describe how these InfoSec teams have built partnerships throughout the organization. One interviewee explained: "Information Security enables the business to grow, but grow securely."

Practice #1: Build the Business Case

We observed that companies with mature and effective programs to address insider threats approached it as a partnership effort, working directly with the R&D, finance, or whatever business unit had concerns around sensitive data. Specifically, they worked closely with the business unit(s) to understand and identify a tolerance for risk, and to continually develop a case for security that was appropriate to that risk. In other words, security would collaborate to develop an acceptable insurance plan needed to help mitigate against an insider threat.

However, building the business case wasn't a document that said, "we're at risk." Many enterprises already perform such exercises. A risk document was only a part of the process, a small part. Building the business case, for thought leaders, focused mostly on the process of building a case to make the business units better comprehend the risk. The companies in our group use several common approaches and activities to gain the attention of their non-security colleagues:

Practice #1A: Make Security a Revenue—not a Cost—Center

More and more, enterprises recognize that they operate in a world where connectivity is high. Not surprisingly, in 2012, data security was earmarked as the most important corporate priority by 48% board members of and 55% general counsels.[3] In our group, many firms successfully took advantage of this new reality by elevating their roles from technical security to business security.

Traditionally, security is typically classified as a cost center due to its technical nature. However, outlier teams successfully positioned themselves as the guardians of data and intellectual property, helping assure normal business operations.

Practice #1B: Make it Personal

A key finding is that this approach makes it personal: InfoSec discussed the impact of a "worst case" insider breach to the team and the people in the unit, as well as to the larger organization. In this way, InfoSec became very familiar with the operations of the business and the concerns of each business unit and the people who ran it.

Practice #1C: Use Anecdotes

We noticed that InfoSec often used anecdotes to personalize the threat. For example, InfoSec at a medical device manufacturer told the story of how a leak of the company's intellectual property would lead to a shutdown of manufacturing. The story drove the point home, to raise awareness and help change behavior.

[3] http://www.fticonsulting.com/global2/media/collateral/united-states/legal-risks-on-the-radar.pdf

"A few smart companies have stopped complaining about SOX and turned it to their advantage—bringing operations under better control while driving down compliance costs."

– Harvard Business Review, 2006

Practice #1D: Leverage Compliance for Security

We found that companies who were successful at addressing insider threats had a strategic attitude about compliance instead of a "checklist" attitude. They embraced it, and used as a driver to bolster their security initiatives and differentiate their businesses.

Although compliance doesn't guarantee perfect security, it helps the odds dramatically. And buy-in on compliance from the top increases the success of compliance efforts, and therefore of security against insider threats.

Practice #1E: Create a Network

As InfoSec creates informal teams and relationships throughout the company, it becomes familiar with the roles and operations of the business in every business unit. As a result of their involvement, security initiatives and awareness pervade the organization. InfoSec becomes part of the corporate DNA. Business units willingly work with InfoSec to understand and mitigate their risks. Ideally, business units proactively seek out InfoSec before making decisions.

Practice #1F: Heavy Use of Analytics

Advanced organizations use security analytics. Analytics serve two main functions:

- With the growth of bring your own device (BYOD), tracking and managing devices has become impossible. However, analytics can help identify aberrant data and intellectual property access.
- Combat advanced threats coming from governments. Though not related directly to malicious insiders, for many enterprises, analytics helps provide the incite needed to identify advanced threats.

Practice #2: Organize for Security

We observed two organizational models that effective InfoSec teams follow. Initially, security teams followed a centralized organizational model. Roles within a centralized team can be diverse, and responsibilities can span the entire organization. For example, one person may be in charge of security in web apps, and another for sharing information with third parties.

A unified team has its advantages and is often the most sensible approach in the smallest companies. On the con side, centralized teams tend to get less budget and visibility, and can even be viewed as detached.

Over time, especially with larger organizations, especially with multiple geographies or lines of business, InfoSec staff tends to be embedded in the business units.

The advantages of the decentralized model are higher involvement and visibility, and therefore a higher budget. The disadvantage is that roles between business units can easily become redundant, and InfoSec professionals on different teams can even come to crossed purposes. Regardless of organizational method, we noted two distinct practices:

Practice #2A: An Integrated Security Organization

Advanced organizations were marked by a broader integration with other security-related disciplines, especially fraud and privacy. This integration underlies the role of business security over technical security.

Practice #2B: Adopting an Assurance Model

Advanced organization put in place security policies, deploying a consistent cycle of inspection and verification. By contrast, many other firms today relied on a trust but don't always verify approach.

Practice #3: Work with Human Resources

The power of HR to create a security-minded culture can't be overstated. Duke University Professor Dan Ariely conducted experiments on students doing a math exercise in which they report their own scores. Typically, a moderate number cheated on the exercise to collect a small prize. But when students were reminded of the Ten Commandments before the exercise, or asked to swear on a Bible, even among self-declared atheists, cheating dropped to nearly zero.[4]

"While ethics lectures and training seem to have little to no effect on people, reminders of morality—right at the point where people are making a decision—appear to have an outsize effect on behavior."

– Dan Ariely, James B. Duke Professor of Behavior Economics at Duke University

We observed a very tight integration between InfoSec and HR among companies that deter insider threats using a variation of Dr. Ariely's prescription. While it's common for HR and InfoSec to work together for employee onboarding and offboarding, these companies had built a richer relationship (in fact, on- and offboarding were typically automated). The real relationship centered around HR's ability to communicate InfoSec's requirements and expectations, and create an atmosphere that supports data security and respect for corporate digital assets. In these companies, HR was an effectively InfoSec spokesperson. The key practices used by our group:

Practice #3A: Onboard with Security in Mind

HR also supported InfoSec in its onboarding practices, beyond the typical background checks. InfoSec worked with HR to develop psychological testing methods to evaluate candidates, and many added additional testing and evaluation of executives. One company made a point to instruct new hires not to bring competitor data, demonstrating that the reverse would not be tolerated when they leave.

Practice #3B: Elevate Violations to HR

The companies we surveyed employed the clout and authority of HR to handle violations of security processes, making it clear to all employees that insider security infractions have disciplinary consequences. In one large insurance firm, HR has direct access to incident reports of security breaches, so that they have the entire dashboard for making disciplinary decisions.

Practice #3C: Automate Termination Processes

Most of the companies in our survey automated their termination processes to shut down access to data quickly and completely. Successful implementation of this automation is made possible when InfoSec and HR have a tight integration.

Practice #4: Work with Legal

Companies who participated in our survey also had a tight integration between InfoSec and the Legal department. Where security is concerned, Legal's role is similar to HR's: to use its clout and authority to create a business culture where the consequences of internal breaches are well known.

While, for many firms, this means following the compliance checklist, we found advanced companies using Legal in innovative ways.

Practice #4A: Approve Security Policies

Legal works with InfoSec to develop and approve basic security polices for the company, including usage of email, networks, and social media, care of laptops and other portable devices, and the monitoring of user behavior. To whatever extent these measures are appropriate in each company, the clout of the Legal department legitimizes employee policies.

[4] Dan Ariely, "Why We Lie," The Wall Street Journal, May 26, 2012. http://online.wsj.com/article/SB10001424052702304840904577422090013997320.html

Practice #4B: Communicate Scary Legal Policies

When employees know that their employers have strict legal policies and are ready to enforce them, behavior changes. The companies we studied clearly communicated their legal policies and involved Legal in enforcement to add a "fear factor." For example, a banking company sent each departing employee a list of all company data they accessed in the last six months. Legal then used this list to send both the departing employee and their new employer an official warning letter, letting them know that the company was watching for signs of their data falling into a another company's hands.

Practice #4C: Review Third-Party Contracts

Our companies recognized that their partners could be a significant source of insider threats. By working closely with InfoSec, Legal was able to tighten up contracts. Partners then had an obligation to manage data access to the same standards as the partnering company. These agreements are particularly important in setting terms with consultants who will work on-site or have virtual access to data, or relationships in which sensitive data is shared between firms.

Practice #5: Educate

Every InfoSec team needs to be educated about insider threats, but for our group, the education extends to employees in a very concerted manner.

"Although it is obviously important to pay attention to flagrant misbehaviors, it is probably even more important to discourage the small and more ubiquitous forms of dishonesty—the misbehavior that affects all of us, as both perpetrators and victims. This is especially true given what we know about the contagious nature of cheating and the way that small transgressions can grease the psychological skids to larger ones."

– Dan Ariely, James B. Duke Professor of Behavior Economics at Duke University

Practice #5A: Educate Employees Constantly

Our companies conducted regular employee training programs, ideally twice per year for every employee. In practice, bi-annual live training is difficult and expensive, but advanced companies get around the obstacles using email, newsletters, flyers with tips included with pay slips, and poster campaigns in the breakrooms. In these communications, they also made it personal by using real-world, local examples. As a result, these companies created a barrage of information, which demonstrated that insider security was a constant and consistent priority.

The HR departments of companies in our survey developed training and communications programs that consistently reminded employees of their responsibilities to protect the company's security. For example, one company's HR internal communications team would even publish articles in the email newsletter about breaches that took place at other companies, to educate employees on how to avoid similar problems.

Practice #5B: Educate Online

We observed many companies using online security awareness training, typically deployed by HR or Legal. Even small companies are now using the online tools available, to educate employees on policies and best security practices, and to conduct tests on the information. From a legal standpoint, the online tools provide the company with an official record of what they knew and when they knew it, which eliminates the excuse, "I didn't know that was a policy," in case of an infraction.

Practice #5C: Teach Personal Cyber Security

Individuals are concerned with privacy and data security in their homes and for their families, and one company in our study built upon that concern to educate its employees. They provided a personal cyber security class that followed the same principles as the company's internal security policies and worked in information about the corporate requirements. Employees were motivated to attend and put what they learned into practice, thus making both their homes and offices safer. In the bargain, the company built goodwill and trust by offering valuable information.

Practice #5D: Educate InfoSec

The InfoSec teams of secure companies are persistent about attending conferences and professional training. They actively stay ahead of the curve in their professional training.

Part 2: How to Prioritize the Initiatives

Information security is a complex undertaking. The effective InfoSec teams we found, across the board, knew how to prioritize their security initiatives.

Practice #6: Size the Challenge

The companies we studied are good at sizing the challenge. They take a hard look at every possible threat and have innovative ways of collecting and prioritizing their requirements

Practice #6A: Identify the Threats

We observed companies making detailed inventories of the assets that are subject to a breach, and the possible ways they could be breached. One interviewee told us: "We start by identifying what makes our company unique." That is, they focus first on the assets that are most likely to be targeted. Their inventories include all the threats identified in our definition of the "insider threat": malicious intent, accidents, and victimization from outsiders.

Practice #6B: Build an Insider Inventory

Sizing the insider threat means sizing the population of insiders. This population includes not only regular employees, but also transient, remote, and mobile workers, and those affiliated with partners.

Partner profiling is particularly important, and sometimes complex, because security standards vary from organization to organization, and partners tend to come and go. For example, the healthcare industry is a network of hospitals, doctors, pharmacies, and insurance companies that share sensitive customer data, and whose relationships change regularly. Every data transaction is a potential breach. For example, recently a spreadsheet of health information was accidentally posted on the Internet when one partner shared it with another.

Practice #6C: Map the Threats

The next step is to map the insider inventory against the possible threats. Some teams created a matrix on a spreadsheet of every known asset and every insider group that could commit a breach on that asset. The result is a comprehensive list of what-if scenarios that forms the basis of a prioritized plan.

With this inventory in hand, the InfoSec team can account for audit and visibility requirements, to ensure that data is accessible to those who need it, and inaccessible to those who don't.

Practice #6D: Classify Sensitive Information

Identifying the information within the corporate databases and file servers allows understanding of risk and severity of data access.

Practice #6E: Analyze and Audit Activity

By keeping track over access and access patters, it becomes very easy to understand who accessed your data, what was accessed and why.

Practice #7: Start Small, Think Big.

Once they identified all the possible scenarios, companies in our study used their matrix to prioritize.

Practice #7A: Consider the Consequences

One company in particular used this list to brainstorm, with the business units, the consequences of every possible breach. For example:

- Would it drop the stock price?
- Give an advantage to a competitor?
- Break a government regulation?
- Threaten a customer's privacy?

The severity and likelihood of these consequences helped them set their priorities.

Practice #7B: Don't Get Overwhelmed

For an organization of any size, a list of every breach scenario could be an overwhelming amount of data. No InfoSec team can secure everything at once. The key is to start with the most basic priorities, to put a lock on the "jewelry box" instead of building a wall around the entire house.

Successful teams realized that doing too much, too soon, would not only put unrealistic demands on themselves, but would be disruptive and confusing to the business units they serve. Instead, they started with small but significant victories, based on a prioritized plan.

Practice #8: Automation

Deciding what to automate goes hand in hand with prioritizing. Effective InfoSec teams used the prioritization process to drive automation, rather than resorting to any vendor technologies that may be available.

These are the automated systems we observed consistently among the companies we studied:

- **Online training:** As explained above under "Educate Online," online training tools maximize the reach of the security education program.
- **System inventory:** Automated tools were used to inventory assets in the discovery process.
- **Fraud prevention**
- **Provisioning and de-provisioning privileges:** These systems reveal who has access to what data and whether they log in, enable reviews of access privileges, and clean up dormant accounts.
- **Onboarding and offboarding:** These systems grant and remove privileges automatically; they are particularly useful when employees depart, giving HR immediate control to remove permissions.

Part 3: Controlling Access

Access controls formed the backbone of an insider threat strategy on many levels. With the disintegration of the perimeter, less, sometimes zero faith was placed in filtering systems designed to identify and stop sensitive content from leaving the premises. With Prussian-like precision, security locked down data and other content with a set of access control systems.

Practice #9A: Guard the Guards

The first step: Lock down admins and super users. Administrators and other super users have often been the first to violate security by accessing things they shouldn't. Recently, we are seeing this replayed today with the growth of SharePoint, for example. The Register reported on a survey on SharePoint admins, finding that the "most popular documents eyeballed were those containing the details of their fellow employees, 34 %, followed by salary—23%—and 30% said 'other.'"

Our firms typically implemented three practices:

- Sensitive transactions should require additional approval to prevent fraud
- Separate policy for privileged users
- Privileged user monitoring

Practice #9B: Co-manage Access Rights with Lines of Business

Firms in our group put in place a detailed permissions structure that is comprehensive and flexible. A key activity: permissions discovery, a simple but comprehensive inventory of who can see what. Over time, the notifications were put in place that recognized key events such as:

- Job changes
- Terminations
- Sensitive transactions should require additional approvals to prevent fraud
- Unusual access attempts
- Repeated attempts

Security teams, unaware of day-to-day business events, put business owners in charge of verifying access rights. This also included setting timetables for reviewing access rights.

Practice #9C: Focus on Identifying Aberrant Behavior

At Black Hat USA 2012, Jonathan Grier described how studying statistical aberrations when it came to accessing files helped identify insider threats when it came to forensic analysis.[5] The same can apply as an insider theft occurs. Bradley Manning, the US Army private who accessed and provided sensitive Department of State documents to Wikileaks, accessed thousands of documents using a script that downloaded files from SharePoint at inhuman volumes. Weirdness usually means trouble.

In our group, profiling normal, acceptable usage and access to sensitive items is a key part of mitigating insider threats. Typically, profiling would focus on, as one participant put it, "cameras in the vault." The cameras looked for aberrations in:

- Volume
- Access speed
- Privilege level
- Checking the entry method—Legitimate individuals should, typically, access data through a main door.

[5] https://www.blackhat.com/html/bh-us-12/bh-us-12-archives.html#Grier

Most firms we profiled recognized that nothing will stop the proliferation of mobile computing devices (also known as the consumerization of IT). But they recognized that it doesn't matter so much what device you use vs. how employees interact with the data. That's where identifying aberrant behavior is essential. Whether you're accessing thousands of records via iPad or PC makes little difference: it's still aberrant. Most participants emphasized that in the case of a lost or stolen device, remote wipe is very important.

Part 4: Implementing Technology

Firms in our group would pick technologies that were mapped to mitigating threats, but would constantly engage in a process of readjustment. This rebalancing of the technical portfolio would take place annually, with security assessing what was needed, what was working, and where future threats could come.

The typical technologies deployed varied widely among our small sample size, making it difficult to identify specific trends. Since the technologies are basically the technical solutions to address the different practices, the question then boils to how to choose what's right for a particular enterprise.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.