



---

**The OneSign™ Guide to  
Thwarting Insider Threats**



## TABLE OF CONTENTS

---

Facing the Reality of Internal Risk.....	2
The Face of the Insider Threat.....	2
How OneSign Supports Carnegie Mellon’s Best Practices.....	3
Beyond Insider Threat Best Practices.....	7
Learn More.....	7

## Facing the Reality of Internal Risk

---

When we think about IT saboteurs, most of us picture a professional cyber-criminal or hacker bent on stealing confidential information or wreaking havoc. In both cases, the perpetrator is an outside party who breaches the data network of a company, institution, or government entity with malicious intent. In response to this perception, companies have implemented layers of physical and IT security around the perimeter of their organizations—and yet we are still vulnerable as evidenced by the number of IT incursions we see every day.

Truth is, the reality of IT sabotage is more complex. According to one survey conducted in 2004, 29% of “e-crime” attacks were known to have been perpetrated by insiders—typically employees, former employees, or contractors. Most often, they are people who, at one time or another, were on the payroll of the organization and have an intimate knowledge of the security systems and policies in place. Another study published recently in the *Journal of Computer Mediated Communication* stated that about 80% of publicized data breaches in 2006 came from internal sources, up from more than 50% a year earlier.

Those rising percentages may be a reflection of the success organizations have had in thwarting external threats. In recent years, advances in perimeter security technology—such as packet filters and intrusion prevention and detection tools—have enabled organizations to reduce the risk of external network attacks. However, most companies have done little to counter internal threats—threats that can be even more damaging to a company’s business and reputation, exposing lax policies and inadequate management.

Fortunately, there are ways to combat the insider threat—effectively and affordably—and the Imprivata OneSign Platform can play a prominent role.

## The Face of the Insider Threat

---

In May of 2005, the U.S. Secret Service and Carnegie Mellon University’s Software Engineering Institute published a study entitled *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. (This study is available for download in PDF format at [http://www.cert.org/insider\\_threat](http://www.cert.org/insider_threat).) The study analyzed the insider threat, including profiles of attackers and their motivations and recommendations for the prevention of attacks.

The study reveals the following key findings about insider attackers and their impact:

- Most attackers are former employees who had held technical positions with the targeted organizations;
- Most attacks are perpetrated against private sector organizations;
- Insider attacks cause organizations financial losses, negative impacts to business operations, and damage to reputation;
- Most insiders involved are charged with criminal offenses based on violations of federal law;
- Most insider actions are triggered by a negative work-related event;
- The majority of insiders plan their activities in advance;
- When hired, the majority of insiders were granted system administrator or privileged access, but less than half of all of the insiders had authorized access at the time of the incident;
- The majority of insiders compromise computer accounts, create unauthorized backdoor accounts, or use shared accounts in their attacks;
- Remote access is used to carry out the majority of attacks;
- The majority of insider attacks are only detected after a noticeable irregularity in the information system or system unavailability.

These findings suggest that the insider threat can be substantially reduced if organizations take measures to deter attacks from happening in the first place and to respond swiftly and effectively if they do.

## How OneSign Supports Carnegie Mellon's Best Practices

---

Following the insider threat study prepared by the U.S. Secret Service and Carnegie Mellon University's Software Engineering Institute, the University's CyLab organization published a report, entitled *Common Sense Guide to Prevent and Detection of Insider Threats*, outlining 13 best practices to help organizations avoid insider threats. (This report is available for download in PDF format at [http://www.cert.org/insider\\_threat](http://www.cert.org/insider_threat).)

Of the CyLab's 13 recommendations, 10 best practices can be supported—in whole or part—by Imprivata® OneSign™ solutions. The following discussion analyzes those 10 practices and the key role Imprivata OneSign solutions can play in their implementation:

### ***PRACTICE 1: Institute periodic enterprise-wide risk assessments.***

Before an organization can defend itself against insider attacks, it needs to understand its vulnerabilities. The CyLab report recommends identifying critical assets, then developing a strategy to protect them following risk management principles. Key to this effort, according to the report, is taking "an enterprise-wide view of information security." We at Imprivata recommend going one step further and taking an enterprise view of all security—both information (logical) and physical security—to understand how they reinforce each other's effectiveness in countering insider threats. This is because often the vulnerabilities that malicious insiders exploit result from a lack of integration between physical and logical security.

For example, insider attacks commonly occur after an employee has been terminated from work following a performance or behavior issue. While that employee's physical access to the facility is usually immediately suspended by the physical security department with all badges and access cards surrendered, it can often be days or weeks before the IT department removes the user's information access privileges. That lag time gives the disgruntled former employee plenty of opportunity to plan and execute a malicious attack via remote access.

**The solution:** OneSign Physical/Logical integrates building and network access systems for unified enterprise security management. Beyond simply leveraging the building access badge, OneSign Physical/Logical consolidates electronic identities between physical access systems and IT directories to enable one converged policy for allowing or denying network access based on a user's physical location, role, and/or employee status. When an employee is terminated, user privileges are immediately revoked, thereby preventing a post-employment insider attack.

### ***PRACTICE 2: Institute periodic security awareness training for all employees.***

No organization's data can be safe if its employees don't take security seriously. Periodic security awareness training can alert employees to the security risks and their responsibility to safeguard their organization's critical assets. This training may also help prevent insider attacks by reminding potential attackers of the policies, procedures, and technical controls the organization has in place to detect, deter, and respond to insider threats.

However, a culture of security awareness can only go so far to prevent insider attacks. Even security-conscious employees may become lax in their habits if their security-related responsibilities become too burdensome. For example, strong password policies are seldom effective when employees are required to manage and change complex application passwords on a regular basis. Users resort to writing passwords down and leaving them in plain view where a malicious attacker can find them and use them to gain unauthorized access. Therefore, it is essential to reinforce security awareness with systems that make users' security responsibilities easy to fulfill.

**The solution:** OneSign Single Sign-On makes it easy for users to comply with strong password policies, because it replaces multiple application passwords with a single complex password that can be changed

periodically according to the policy. OneSign Single Sign-On also dramatically lowers Help Desk costs associated with forgotten password resets, increases user productivity and satisfaction, and supports regulatory compliance initiatives. With OneSign Single Sign-On, users can keep their passwords secret and thereby reduce the insider threat. When an organization takes proactive steps to deal effectively with the increasing number of passwords and accounts and introduces strong authentication measures, it puts users on notice that security is taken seriously. Organizations seeking a more comprehensive level of security may opt to implement OneSign Physical/Logical, which can be configured to require users to swipe their access cards on a door entry reader before logging onto a computer. Besides strengthening security, this requirement reminds users that they play a major role in maintaining a secure IT environment.

***PRACTICE 3: Enforce separation of duties and least privilege.***

This practice is based on the idea that the more critical responsibilities are divided among multiple employees, the lower the risk that any one person can perpetrate a crime. One way to separate duties is through “least privilege”—a concept whereby all employees are only authorized to access the absolute fewest online resources they need to do their jobs. The best way to implement least privilege is through role-based access, where access to certain applications and information is restricted to only those employees in certain roles.

Role-based access and least privilege have been part of physical security practices for years. For example, many companies restrict access to certain high-security areas of their buildings, such as R&D labs or data centers, through the use of access cards. Now, organizations can extend the practice to IT security through the use of technology solutions.

**The solution:** The OneSign Platform can play a significant part in enabling role-based access and least privilege. OneSign Authentication Management makes it possible for organizations to replace Windows and remote access VPN passwords with a broad range of strong authentication options, including finger biometrics, smart cards, proximity cards, USB tokens, and One-Time-Password tokens—including VASCO Digipass. During setup, security administrators can readily assign access rights to groups of users or even individual users based on their roles within the organization. OneSign Single Sign-On can extend this same role-based access policy to applications, controlling what applications are SSO-enabled. OneSign Physical/Logical takes it one step further by integrating building and network access systems to allow organizations to grant or deny network access based on a user’s physical location, role, and employee status. For example, organizations can configure OneSign Physical/Logical to restrict access to critical applications to only specific computers in work areas secured through the use of appropriate card types. By linking IT or application access to a physical location, OneSign Physical/Logical offers organizations an effective means to tie a user’s logical access rights to role information assigned by the physical access system.

***PRACTICE 4: Implement strict password and account management policies and practices.***

As noted above, strict password policies are a highly effective way to minimize unauthorized access to networks and applications—but only if users can comply with the policies without having to change their behavior. Implementing password policies to improve password complexity or frequency of change can often backfire and reduce security as users get fed up and jot their passwords down on paper placed strategically around the work area. That’s why a single sign-on solution is essential.

**The solution:** When organizations deploy OneSign Single Sign-On, they can set parameters for password complexity, frequency of password changes, and more. The solution is virtually transparent to users, so compliance is assured. OneSign Single Sign-On is a centrally managed solution, which makes it easier for organizations to establish and maintain stringent account management policies and practices.

***PRACTICE 5: Log, monitor, and audit employee online actions.***

The only reliable way to associate online actions with the employee who performed them is to enforce account and password policies or use strong authentication such as tokens, biometrics or facility access badges. Otherwise, potential inside attackers can hijack other users' accounts, assume their coworkers' identities, and leave no telltale traces behind after they've inflicted their damage. The best way to enforce policies reliably is through use of strong authentication combined with single sign-on. The single sign-on solution should have a robust auditing function so that security personnel and system administrators can track user behavior and spot any suspicious activity.

**The solution:** The OneSign Platform helps ensure that all users are reliably identified and their activities logged. It supports shared workstations and automatic log-offs, so that even the behavior of employees who share a single PC can be reliably tracked. The OneSign Intelligent Agent allows organizations to monitor, capture and log password-related application access events in a centralized database. Easy-to-use detailed reporting can strengthen security and enforce regulatory compliance across all applications. Administrators can easily monitor access records for every user, application or workstation in one, central location—even revealing users that may be sharing credentials to confidential applications.

OneSign Physical/Logical allows even more detailed auditing and allows the user's physical presence in the work area to be stored as part of the audit record. The ability to link the electronic identity used to log-on to an application to a specific access card used to gain entrance to a building or work area has tremendous deterrence value, as it prevents users from hiding behind the anonymity of an electronic log-on.

***PRACTICE 6: Use extra caution with system administrators and privileged users.***

The majority of insiders who commit sabotage or steal confidential information are people in technical positions with greater access to applications and systems and the necessary expertise to inflict damage and cover their tracks. To minimize risks, no single user should be permitted or be technically able to release changes to the production environment without online action by a second user. This can prevent an insider from releasing a logic bomb without detection by another employee. In addition, since many malicious insiders are former employees who launch their attacks shortly after termination, it is essential for organizations to disable the access of privileged users immediately after they are discharged.

**The solution:** OneSign Physical/Logical consolidates identities between physical access systems and IT directories to enable one converged policy for allowing or denying network access based on a user's physical location, role, and/or employee status. When an employee is terminated, user privileges are immediately revoked, thereby preventing a post-employment insider attack.

OneSign can also be effective against abuses of administrative passwords that are shared among multiple privileged users. While it is common practice to disable the primary network accounts for the administrator upon employee termination, what is often unknown are the credentials the terminated user had in common with other administrators. With OneSign Single Sign-On, a report can be generated showing the number of users and applications those users have in common.

***PRACTICE 8: Use layered defense against remote attacks.***

As the Secret Service/Carnegie Mellon study revealed, the majority of insider attacks are performed via remote access. Disgruntled insiders must not be given an opportunity to wreak havoc on systems after they leave. Therefore, remote access policies and procedures must be designed and implemented very carefully.

**The solution:** OneSign operates both as a Radius Host and a Radius proxy to help secure remote access through IPsec or SSL VPN gateways. This allows organizations to make remote access policies as stringent as they deem necessary, and to deny access—both direct and remote—to any suspected insider quickly and easily. OneSign Authentication Management can require users to employ a second form of strong authentication, such as a One Time Password (OTP) Token when they log in remotely. That requirement

can be placed on all employees or only those with privileged access or particular roles. An even more comprehensive remote access solution can be implemented using OneSign Physical/Logical to check card holder status before granting remote access. By enabling organizations to terminate both physical and logical access at once, it closes the window of opportunity that otherwise would allow a former employee to exact revenge via remote access. This step is often considered critical in ensuring that vital gateways into the organization are closed.

***PRACTICE 10: Deactivate computer access following termination.***

Organizations need to establish and consistently follow a termination procedure that quickly disables the terminated employee's access to everything—physical locations, networks, systems, applications, and data.

**The solution:** The latency in terminating access often allows disgruntled employees either to return physically into the facility ("tailgating" behind another employee) or to gain access remotely. The OneSign Platform prevents this by making it easy for organizations to swiftly and effectively disable access. In addition, only OneSign gives organizations the power to lockout remote, network, and application access once the user's facility access is terminated. This lockout instantaneously occurs without the need for either the manual or automated workflow that many organizations commonly follow.

***PRACTICE 11: Collect and save data for use in investigations.***

Hard evidence is essential to successful identification of suspected insiders and subsequent prosecution. Organizations must have a mechanism in place to collect and save all relevant data.

**The solution:** The OneSign platform automatically tracks user activity and saves all audit information within its own database to protect them from being electronically modified. This is a critical weapon in the arsenal against insider threats because it protects the data from being changed even by an administrator. Built-in reporting tools can help organizations do forensic work and quickly sift through historic data to spot suspicious behavior.

***PRACTICE 12: Implement secure backup and recovery processes.***

If an insider attack causes extensive damage, it is essential that organizations have secure backup and recovery processes in place to restore systems quickly and minimize business disruption and further damage.

**The solution:** The OneSign platform includes redundant systems and backup and restore capabilities to preserve data in the event of a system failure. This helps ensure that any data that can trace the insider to the sabotage or theft remains available to help solve the crime and aid in prosecution.

## Beyond Insider Threat Best Practices

---

The Imprivata OneSign platform is a powerful weapon in the fight against insider threat, but its value goes well beyond that one area of concern. The added benefits of OneSign products include:

***Simplified password administration.***

With OneSign Single Sign-On, administrators can implement a straightforward password policy across all applications based on users' primary authentication. To increase password security, OneSign can cycle application passwords behind the scenes and disable any user with a single mouse-click.

***Reduced help desk costs.***

When users have multiple application passwords to remember, they often forget them – leading them to call their IT help desks for assistance. According to industry analysts, more than 30% of help desk calls are password-related. With a single help desk call costing an estimated \$25, the annual cost of password problems can be considerable. OneSign can reduce the number of help desk calls and the resource costs associated with them.

***Increased user productivity.***

With OneSign Single Sign-On and OneSign Authentication Management, users can gain more immediate access to the applications they need to do their work, and spend less time tracking down forgotten passwords.

***Better regulatory compliance.***

The OneSign Platform supports many of the user authentication, information access control and reporting requirements of government and industry regulations, such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, and HIPAA.

## Learn More

---

For more details on Imprivata's Converged Identity and Access Management Platform - OneSign, please visit <http://www.imprivata.com> or contact Imprivata at 877-ONESIGN.

To learn more about the insider threat research conducted at Carnegie Mellon University's Software Engineering Institute, including free, downloadable copies of *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* and the *Common Sense Guide to Prevention and Detection of Insider Threats*, please visit: [http://www.cert.org/insider\\_threat](http://www.cert.org/insider_threat).







10 Maguire Road  
Building 4  
Lexington, MA 02421  
v 781 674 2700  
f 781 674 2760

**Imprivata EMEA**  
Forsyth House  
77 Clarendon Road  
Watford  
Herts, WD17 1LE  
United Kingdom  
v +44 (0)1923 813 511  
f +44 (0)1923 813 501

**Imprivata APAC**  
#01-03 60 Cambridge Road  
Singapore 219757  
v +65 82 004 840

**1.877.ONESIGN**  
[www.imprivata.com](http://www.imprivata.com)  
[sales@imprivata.com](mailto:sales@imprivata.com)