Software Engineering Institute

Best Practices Against Insider Threats in All Nations

Lori Flynn
Carly Huth
Randy Trzeciak
Palma Buttles

August 2013

TECHNICAL NOTE
CMU/SEI-2013-TN-023

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0000570

Table of Contents

Abstract

Based on its analysis of more than 700 case studies, the CERT® Insider Threat Center recommends 19 best practices for preventing, detecting, and responding to harm from insider threats. This technical note summarizes each practice, explains its importance, and provides an international policy perspective on the practice. Every nation can use this paper as a succinct educational guide to stopping insider threats and an exploration of international policy issues related to insider threats.

Introduction

The CERT® Insider Threat Center defines an insider threat as a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, and intentionally exceeds or uses that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems [Silowash 2012]. Based on its analysis of more than 700 insider threat cases mainly from the United States, the CERT Division recommends 19 best practices, adapted from the forthcoming *Common Sense Guide to Mitigating Insider Threats, 4th Edition* [Silowash 2012], for preventing, detecting, and responding to insider threats. This paper maps these practices to international issues that affect practice implementation. Any nation can use this mapping as an educational guide to preventing insider threats and as a preliminary exploration into international security policy issues related to insider threats. We present this paper as an initial discussion of the effects of the international landscape on the implementation of insider threat best practices.[1]

® CERT is a registered trademark owned by Carnegie Mellon University.

[1] The materials presented in this technical note are provided for informational purposes only. These materials are not offered as and do not constitute legal advice or legal opinions. This technical note should not be used as a substitute for the advice of a licensed legal professional.

Best Practices and International Policy Considerations

Practice 1: Consider threats from insiders and business partners in enterprise-wide risk assessments.

Enterprise-wide risk assessments help organizations identify critical assets, threats to those assets, and the mission impact of successful attacks. They also determine which controls to implement to identify and minimize critical risks.

Too often, organizations focus their efforts on physical and technological means of protecting information systems from outsiders but disregard the threat posed by trusted insiders. Insiders are likely to know where high-value information is stored; know about the organization's IT and physical systems; have authorized access to IT systems; and have the trust of co-workers, which makes social engineering attacks more likely to succeed. Physical access to data systems could enable an insider to place keystroke loggers, steal devices, or exfiltrate data. Using authorized access, an insider could copy electronic documents to removable media to steal intellectual property (IP), sabotage data systems, or commit fraud by using personally identifiable information (PII) stored on the organization's systems. Organizations should use defense in depth, in the form of physical and technological controls, to protect critical assets from insiders. Organizations should also require all employees, contractors, and trusted business partners to sign nondisclosure agreements (NDAs) and undergo background checks; contractors' and trusted business partners' background checks should be commensurate with the organization's.

International Considerations

The utility of background checks and contracts such as NDAs or service level agreements (SLAs) may vary per country. Some countries do not have well-developed legal [CIA 2013a] and law enforcement systems, with too few regulations or too little enforcement for contracts to be meaningful [CIA 2013b]. Local background checks (or the entire output of a risk assessment) from a country known for corruption [Transparency International 2011] may not be reliable. Particular indicators of heightened insider threat risk for an individual, such as violating a company policy or having a past court conviction, might correlate differently to insider threat risks in different countries.

Organizations should consider culture when implementing insider threat practices. Culture incorporates all attributes required for humans to adapt to their social and physical environments. Insider threat indicators may vary between cultures and subcultures, some of which span multiple countries. For instance, tardiness at work or missed project deadlines might have different correlations to insider threat in polychronic cultures, which view time as "adjusted to suit the needs of the people," than in monochronic cultures, which place a high value on adhering to schedules [Hall 1959].

Practice 2: Clearly document and consistently enforce policies and controls.

Clear and consistently enforced policies and controls may reduce the likelihood that an insider will feel unfairly treated. Employees are more likely to correctly and consistently follow policies

and controls that are clearly documented (precise, concise, and coherent), are consistently enforced, are available for reference, and include the reasoning behind the policy and the ramifications of policy violation. Employees should sign off to confirm understanding of policies and commit to abide by them, upon hire and regularly thereafter. Organizations should be particularly clear on policies regarding acceptable use of the organization's systems and data, ownership of work products, evaluation of employee performance, and addressing employee grievances.

International Considerations

Communication of policies and controls should account for cultural differences and attributes such as low- or high-context communication. Low-context cultures communicate in explicit ways. High-context cultures communicate in implicit ways, relying on a presumed context of cultural information to fill in the gaps [Hall 1959].

Factors affecting consistent enforcement of policies and controls include a nation's regulations, law enforcement, and corruption, as discussed in Practice 1. Requirements for employee consent vary by nation; for example, the European Union appears to have a stricter standard DPWP 2011] than the United States.

Practice 3: Incorporate insider threat awareness into periodic security training for all employees.

Periodic security training for employees raises awareness of risks to the organization, potential targeting of employees for criminal recruitment, and ways to protect critical assets. Organizations should train their employees to recognize insider threat behavior such as unauthorized copying of the organization's data; social engineering attempts to obtain passwords, the organization's information, or unauthorized access to facilities; and threats to the organization or employees. Training should cover procedures for reporting suspicious behavior, and employees should be regularly tested for understanding of the organization's policies.

International Considerations

Respectful and effective methods of teaching and reporting vary by country, culture, and subculture, as discussed in Practice 2. Training styles and content should account for low- or high-context communication styles and other culturally relevant considerations.

Practice 4: Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

Organizations should conduct background checks and periodic reinvestigations on prospective employees, contractors, and workers from trusted business partners to identify insiders' personal, professional, and financial stressors. The content of the background check varies according to local, current laws, but it may include checks for previous criminal convictions, verification of credentials and past employment, a credit check, and competence evaluations from past employers. Organizations should identify risk levels for all positions and more thoroughly investigate individuals applying for or occupying higher risk positions. Organizations must either consistently enforce sanctions for all rule violators or risk emboldening insiders. Responses to

behavioral disruptions include a warning; punitive action; or referral to an Employee Assistance Program (EAP), which might reduce the risk of an insider deciding to harm the organization.

International Considerations

Laws about background checks [Ben Cohen 2010, EEOC 2012] and worker monitoring [Lerner 2012] as well as workers' willingness to report incidents vary widely by country and even region. Some nations' work environments do not protect employees from discrimination by caste [Human Rights Watch, India 2012], gender [UN 2007], race [Wikipedia 2012], and sexuality [UN 2011], and have ineffective legal protections for whistleblowers, if they have such protections at all [Kaplan 2001, OSHA 2013, Collins 2010]. Those work environments may not be conducive to unprotected workers reporting suspicious or disruptive behavior, because the insider or acquaintances might easily take revenge.

Some national cultures have strongly collectivistic or individualistic tendencies [Hofstede 1980]. Collectivists might report security problems for the good of the group, or they might refrain from reporting for fear of hurting the group. Individualists might not report because they see no benefit to themselves for reporting, but they might report to earn small rewards offered for identifying security problems.

Practice 5: Anticipate and manage negative issues in the work environment.

Organizations should clearly communicate expectations regarding acceptable workplace behavior, career development, conflict resolution, work hours, dress code, and other workplace standards. Consistent enforcement of well-documented policies and practices fosters a fair work environment, which may reduce insider disgruntlement. Employees with unmet expectations, such as bonuses, raises, or promotions, sometimes harbor negative feelings. If the organization is not able to provide raises or bonuses in a given time period, advance notice from management may help manage employees' expectations. Clear requirements for advancement and bonuses may also keep expectations in check. Security personnel should be extra vigilant regarding individuals impacted by organizational financial stress or downsizing. EAPs may assist employees with professional and personal stressors, possibly lowering insider threat risks.

International Considerations

This practice shares the communication issues discussed in Practice 2. Expectations vary with different national, cultural, and organizational norms, and organizations should consider normal local expectations when managing possibly negative issues.

Practice 6: Know your assets.

Knowledge of assets is important for information security in general, as well as for recovering from or mitigating potential insider harm. An insider may be less likely to steal IT equipment if assets are documented. Once an organization determines the value of its critical assets, it can implement protections that may be effective against both insider and outsider threats. Organizations should manage all physical and information assets, who has authorized access to them, and where they are located. Organizations should understand the types of data they process and where the data is processed and stored. A physical asset inventory should identify the asset owner's functions and the type of data on the system. The organization should document the

software configuration of all its assets. For servers, the organization should document IT support contacts for each application or database. Assets and data should be prioritized to determine high-value targets. Asset lists should be updated in a timely manner.

International Considerations

Employees in nations that lack legal protections, as discussed in Practice 4, may feel uncomfortable reporting fraud or theft uncovered in the asset documentation process. The trustworthiness and thoroughness of asset documentation depends on national regulations, law enforcement, and corruption, as discussed in Practice 1.

Practice 7: Implement strict password and account management policies and practices.

To compromise accounts, malicious insiders have used techniques such as password cracking, social engineering, creating backdoor accounts, and using shared accounts still available after the insider was terminated. Organizations can impede a malicious insider's ability to abuse the organization's systems by creating password policies and procedures that ensure strong passwords that are regularly changed and forbid sharing passwords. Staff must receive training on these policies and procedures. All staff, including contractors and vendors, should be subject to these policies, and legal counsel should contractually require contractors to provide timely notification of the termination of any of their employees. Organizations should limit the use of shared accounts and periodically audit and re-evaluate the need for all accounts.

International Considerations

Many organizations collect personal data, either about their employees (e.g., social security numbers) or as part of a customer service (e.g., bank account information). In the United States, state and federal government regulations set security requirements for personal information, for example by requiring strong passwords that are regularly changed [FTC 2006]. Many nations have regulations that protect personal data and require appropriate information security, for example, by including password and identification requirements as minimum security measures [Italian Data Protection Authority 2003, Annex B]. The safeguards that are considered appropriate may vary among nations. Organizational culture may also impact this practice, particularly password policy. An organization may have a documented policy on password security but, in practice, allow employees to share passwords. Employees in certain organizational or national cultures may resist strict controls. For example, employees in a collectivistic, cooperative culture may feel strict controls hinder cooperation [Valdez 2009].

Practice 8: Enforce separation of duties and least privilege.

Organizations can use separation of duties and least privilege to limit access to technical systems and physical spaces, limiting the damage a single malicious insider can perpetrate. The two-person rule, enforceable through technical or nontechnical means, requires two individuals to participate in a task for successful completion (e.g., backup and restore functions). The rule of least privilege requires that employees have access only to the resources they need to perform their job. Implementing least privilege is a continuing process because employees experience

change (e.g., promotions) over their employment lifecycle. Role-based access control limits access according to job function.

International Considerations

Industry requirements may affect this practice, for example by requiring the implementation of strong access control measures, including unique IDs and need-to-know access [PCI Security Standards Council 2010], or separation of duties to comply with requirements to manage and control risk [FDIC 2012]. A nation's data protection laws may also require technical and physical access controls [AEPD 1999]. Culture may also be implicated in this practice. For example, in cultures that place a high value on trust, the two-person rule may cause employees to feel that their organization does not trust them.

Practice 9: Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

An organization must ensure its data protection and monitoring requirements for cloud providers are commensurate with the organization's own requirements. Protections include physical and technological requirements, as well as human resources practices for cloud provider employees. Cloud providers should perform pre-hire background checks that are regularly updated after hire, obtain acknowledgement of policies and practices, and provide training on these topics. One potential risk in the cloud environment is the rogue administrator, including hosting company administrators, virtual image administrators, system administrators, and application administrators. These insiders may exploit vulnerabilities in the cloud or use the cloud as an attack platform. Organizations must review the cloud provider's SLA and insurance to ensure that risks and liability are suitably addressed. They must also review the policies and practices of their provider to ensure it is implementing appropriate measures to protect the confidentiality, integrity, and availability of data. The SLA might include the ability to audit the provider, requirements specific to human resources supply chain management, or requirements for security breach notification. The organization, a third party, or the provider itself should continuously monitor the distributed infrastructure, review audit logs, aggregate diagnostic data, and periodically audit the cloud infrastructure to ensure virtual machines and other cloud systems meet security configuration requirements.

International Considerations

Cultural factors of risk determination may affect this practice. Third-party access to an organization's data carries inherent risk, and the organization must decide how much of that risk to accept and how much it can mitigate through contracts, controls, and practices. Also, cloud service providers store data in varying locations, and data protection and data breach laws vary by industry and country. Within the United States, they vary by state, as discussed in greater detail in Practice 7. Organizations must determine how to comply with applicable data protection and breach laws in whatever jurisdictions the cloud service provider keeps its data. Organizations may want to consider controlling the provider's ability to move their data to different jurisdictions, keeping in mind that some jurisdictions' regulations may not sufficiently protect the security or privacy of data. Likewise, statutes and case law in different jurisdictions may affect the enforceability of the SLA requirements outlined in this practice.

Organizations should consider the ownership and privacy of data stored in the cloud. Employees may have certain expectations about the privacy of their cloud data, depending on legal requirements and cultural expectations. Rules about data ownership may vary by jurisdiction, such as when and if a cloud provider can or should relinquish data during an investigation or legal proceeding. Similarly, if a breach does occur, nations may have varying requirements for evidence preservation as well as licensing for computer forensics experts.

Practice 10: Institute stringent access controls and monitoring policies on privileged users.

Privileged users may pose an increased risk to organizations because they have greater access to systems, networks, and applications; technical abilities; the ability to log in as other users; and oversight and approval responsibilities. Malicious privileged users have executed technically sophisticated attacks and concealments, including writing logic bombs, planting viruses, and modifying system logs. To prevent, detect, and respond to malicious privileged users, organizations can consider several different techniques such as nonrepudiation, which allows online activity to be attributed to a single employee. Organizations could require privileged users to sign privilege-specific policies, including user agreements and rules of behavior. It is critical to enforce separation of duties for privileged employees. Finally, organizations must ensure that they have completely disabled access for terminated privileged users; many insider threat cases involve former employees.

International Considerations

The extent to which an organization can implement privileged user policies may depend on national employment laws or even the requirements of a specific industry (e.g., union negotiations). Enforcement of these policies may also depend on the culture of the organization or even the subculture of the privileged users. As discussed in Practice 12, industry or international regulations as well as cultural values can hinder or enhance an organization's ability to monitor its employees.

Practice 11: Institutionalize system change controls.

Many malicious insiders have made unauthorized modifications to organizational systems, such as inserting backdoors. Organizations can use change controls to document changes and safeguard the integrity and accuracy of their systems and data. Organizations must identify and document baseline software and hardware configurations and update this information as changes are made. The change control process must also protect change logs, backups, source code, and other application files. By defining and assigning roles to different individuals throughout the change control process, an organization can make it difficult for a single malicious insider to make undetected changes.

International Considerations

Different international laws may influence data protection through system change controls. Nations may set requirements for personal data, for example by requiring weekly backup copies and the ability to restore data to its original state upon loss or destruction [AEPD 1999], or by requiring that health information is not "improperly modified without detection" [USG 2007].

Practice 12: Use a log correlation engine or Security Event and Information Management (SIEM) system to log, monitor, and audit employee actions.

Organizations can make better informed decisions if they correlate events in their ever-increasing data collection, rather than simply log information. Organizations can use a SIEM system to understand both baseline and irregular activity and to adjust the granularity of monitoring. The development and execution of monitoring policies require input and collaboration from teams across the enterprise, including Legal, Human Resources (HR), and Information Assurance (IA). For example, CERT research has shown that malicious insiders often attack within 30 days of their resignation, so HR should notify IA of pending terminations.

International Considerations

How, when, and what an employer can monitor, in the technical and nontechnical realms, may vary greatly depending on the organization's industry and nation. Culture may greatly influence an organization's decision on what employee information to capture. Some employees may resent an intrusion into information they consider private, while others might not consider that data to be private at all. International laws and regulations may also impact the collection and correlation of employee information, as well as organizations' decisions based on it. Some nations may govern what data employers can collect and requirements for employee notification and consent. However, differences may exist among nations, for example in defining sensitive data [Spring 2012] and in regulating monitoring [ECHR 2007, Wugmeister 2008].

Practice 13: Monitor and control remote access from all end points, including mobile devices.

The increasing trend toward a mobile workforce has also increased the potential for malicious use of mobile devices. Their cameras, microphones, mass storage, and communications capabilities could be used to capture and exfiltrate sensitive information. Organizations must be aware of potential risks posed by mobile application functionality that insiders could use maliciously. A multi-layered defense can include prohibiting personally owned devices, limiting remote access to critical data, limiting the number of privileged users with remote access, and using application gateways for non-organizational equipment. Organizations should more closely log and audit all remote transactions and ensure that remote access is disabled during employee termination.

International Considerations

National laws may affect how an organization uses particular mobile features, for example by recommending that employers adopt geolocation services available on mobile devices "when demonstrably necessary for a legitimate business purpose and the same goals cannot be achieved with less intrusive means" [DPWP 2011]. Cultural norms or laws may also define what monitoring is acceptable for devices that can be used for both personal and work matters [USSC 2010]. Nations may set forth specific requirements for collecting information on remote workers, for example by requiring employers to "ensure that the employees' personality [*sic*] and moral freedom are respected" [Italian Data Protection Authority 2003, Section 115]. Such considerations impact monitoring of system access, especially from mobile devices.

Practice 14: Develop a comprehensive employee termination procedure.

Organizations should develop, communicate, and consistently follow a policy for dealing with voluntary and involuntary employee terminations. All terminated employee accounts must be closed, all organization-owned equipment returned, and all co-workers notified of the departure. Organizations should develop and follow a termination checklist, with an individual assigned to each task, to ensure that the terminated employee's physical and electronic accesses are disabled. Finally, organizations should consider reviewing the departing employee's online actions during the 30 days prior to termination to identify any suspicious network activity [Hanley 2011].

International Considerations

Standard organizational structures vary between countries, as do the set of departments responsible for termination tasks. Laws governing monitoring the online actions of terminating employees and notifying co-workers of the termination vary among jurisdictions. Organizations must consider legal issues surrounding enforcement of agreements on noncompetition, nondisclosure, and intellectual property.

Practice 15: Implement secure backup and recovery processes.

Organizations must have a secure, tested backup and recovery process to ensure compliance with all SLAs. If possible, organizations should implement separation of duties to ensure that a single privileged IT administrator cannot modify the backup and recovery process to prevent the organization from recovering. Transaction logs should be protected so that IT administrators cannot modify logs to obfuscate or delete records of malicious activity. Organizations that rely on a cloud service provider for their secure backup and recovery process should refer to Practice 9.

International Considerations

The availability, variety, and affordability of technical solutions vary among nations of different levels of development. Practice 11's considerations apply here.

Practice 16: Develop a formalized insider threat program.

An insider threat program should be enterprise-wide and establish clearly defined roles and responsibilities for preventing, detecting, and responding to insider incidents. The goal of an insider threat program is to develop clear criteria for identifying insider threats, a consistent procedure for implementing technical and nontechnical controls to prevent malicious insider behavior, and a response plan in the event an insider does harm the organization.

Legal counsel is vital during the information-gathering process to ensure all evidence is gathered and maintained in accordance with legal standards and to issue a prompt legal response when necessary. Legal counsel should also ensure that information is shared properly among the insider threat team members, for instance, to ensure the lawful privacy of employees' mental and physical health information.

International Considerations

There are national differences in the amount and type of employee online activity that can be logged, monitored, and investigated, as well as the circumstances under which it can be done.

International considerations include the need to determine where the incident occurred, if and where the crime could be prosecuted, which law enforcement agency should initiate and conduct the investigation, and which legal statutes should be followed to protect the rights of the accused.

Practice 17: Establish a baseline of normal network device behavior.

Before an organization can differentiate normal behavior from anomalous behavior on networks, it must first capture baseline behavior. A broader approach would also collect nontechnical workplace behaviors. To the extent possible, organizations should collect normal network behavior at the enterprise, department, group, and individual levels. The organization must choose data points of interest, which times to monitor these points for a baseline, and the tools for collecting and storing the data. The longer the organization monitors the chosen data points, the more reliable the baseline is.

International Considerations

Prior to implementing an enterprise-wide monitoring strategy, the organization must consult legal counsel to ensure compliance with international, federal, state, and local laws. Organizations may find it challenging to maintain employee privacy while collecting baseline data.

Practice 18: Be especially vigilant regarding social media.

Organizations should provide training as well as policies and procedures about social media. Such outlets may allow employees to share organizational information that adversaries could use to target current or former employees, either as victims or co-conspirators. For example, attackers might use organizational information to refine spear phishing attempts or fraud schemes. Companies should consider limiting potentially problematic postings on social media, both intentional and unintentional, and developing a social media policy in accordance with applicable laws and regulations.

International Considerations

International considerations related to communication issues surrounding social media sites are similar to training issues in Practice 3. Expectations vary according to different national, cultural, legal, and organizational norms, and organizations should consider local expectations when managing the extent to which employees are permitted to use social networking sites, both inside and outside the workplace, and the degree to which employees are permitted to disclose information about the organization. Some nations do regulate an organization's ability to address employees' behavior online, for example with respect to protected discussions of work conditions [Purcell 2012].

Practice 19: Close the doors to unauthorized data exfiltration.

An organization's first step to addressing insider threats is to identify its critical assets (people, information, technology, and facilities), people who should have authorized access to those assets and those who actually do, and asset locations. To identify risks posed to critical assets, the organization must understand how information assets can be copied or removed. Many technologies and services could be used to exfiltrate data. An organization must be able to account for all devices that connect, physically or wirelessly, to its information system. The

challenge is to balance security with productivity. Controls should allow authorized information exchanges but prevent unauthorized exfiltration.

International Considerations

Availability, variety, and affordability of technical solutions vary among nations of different levels of development. Laws on monitoring and investigations vary among jurisdictions.

Future Work

Planned work includes expanding on the ideas described broadly in this paper to create a detailed international and cross-cultural framework for fighting insider threat. Much work must be done to better understand and characterize different nations' cultural, technical, legal, regulatory, and corruption environments as they affect information security in general and insider threats in particular. Country-specific sets of cases need to be gathered and empirically analyzed for significant correlations between countries and indicators of insider threat risks. The CERT Division has begun collecting international insider threat cases to add to a database originally composed of only cases from the United States, which will help researchers characterize insider threats in various countries.

Bibliography

URLs are valid as of the publication date of this document.

[AEPD 1999]
Spanish Data Protection Agency (AEPD). *Royal Decree 994/1999, of 11 June, which Approves the Regulation on Mandatory Security Measures for the Computer Files which Contain Personal Data.* http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs /reglamento_ingles_pdf.pdf (1999).

[Ben Cohen 2010]
Ben Cohen, Eyal. "Navigating the International Background Screening Jungle Safely and Legally." *EmployeeScreenIQ University*, April 7, 2010. http://www.employeescreen.com/university/ navigating-the-international-background-screening-jungle-safely-and-legally/

[Bishop 2008]
Bishop, M. & Gates, C. "Defining the Insider Threat," article 15. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*. Oak Ridge, TN, May 2008. ACM, 2008.

[CIA 2013a]
Central Intelligence Agency (CIA) of the United States. "Legal System," *The World Factbook*. https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html (2013).

[CIA 2013b]
Central Intelligence Agency (CIA) of the United States. "Economy – Overview," *The World Factbook*. https://www.cia.gov/library/publications/the-world-factbook/fields/2116.html (2013).

[Collins 2010]
Collins, P.; Stein, L.; & Trombino, C. "Consider the Source: How Weak Whistleblower Protection Outside the United States Threatens to Reduce the Impact of the Dodd-Frank Reward Among Foreign Nationals." *The Third Annual National Institute on the Foreign Corrupt Practices Act, 2010*. Perkins Coie LLP, 2010. http://www.perkinscoie.com/files/upload/10_25Article.pdf

[DPWP 2011]
Data Protection Working Party. *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, Article 29*. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (2011).

[ECHR 2007]
European Court of Human Rights (ECHR). *Copland v the United Kingdom* (ECHR 253). ECHR, 2007.

[EEOC 2012]
U.S. Equal Employment Opportunity Commission (EEOC). "Consideration of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act of 1964," *EEOC Enforcement Guidance*. http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm (2012).

[FDIC 2012]
Federal Deposit Insurance Corporation (FDIC). "Section 4.2 – Internal Routine and Controls, Segregation of Duties," *Risk Management Manual of Examination Policies.* FDIC, 2012. http://www.fdic.gov/regulations/safety/manual/section4-2.html

[FTC 2006]
Federal Trade Commission (FTC). *Financial Institutions and Customer Information: Complying with the Safeguards Rule*. http://business.ftc.gov/documents /bus54-financial-institutions-and-customer-information-complying-safeguards-rule (2006).

[Hall 1959]
Hall, E. T. *The Silent Language*. Double Day, 1959.

[Hanley 2011]
Hanley, Michael & Montelibano, Joji. *Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination* (CMU/SEI-2011-TN-024). Software Engineering Institute, Carnegie Mellon University, 2011. http://www.sei.cmu.edu/library/abstracts/reports/11tn024.cfm

[Hofstede 1980]
Hofstede, G. *Culture's Consequences: International Differences in Work-Related Values*. Sage, 1980.

[Human Rights Watch, India 2012]
Human Rights Watch, India. *UN Members Should Act to End Caste Discrimination: More Than 260 Million Affected Worldwide*. http://www.hrw.org/news/2012/05/14 /india-un-members-should-act-end-caste-discrimination (2012).

[Italian Data Protection Authority 2003]
Italian Data Protection Authority. *Personal Data Protection. Legislative Decree No. 196 of 30 June 2003*. http://www.garanteprivacy.it/documents/10160/2012405/ DataProtectionCode-2003.pdf (2003).

[Kaplan 2001]
Kaplan, Elaine. "The International Emergence of Legal Protections for Whistleblowers." *The Journal of Public Inquiry* (Fall/Winter 2001): 37-42.

[Lerner 2012]
Lerner, Carolyn N. *Memorandum for Executive Departments and Agencies*. U.S. Office of Special Counsel, June 20, 2012.

[OSHA 2013]
Occupational Safety & Health Administration (OSHA). T*he Whistleblower Protection Program*. United States Department of Labor. http://www.whistleblowers.gov/ (2013).

[PCI Security Standards Council 2010]
Payment Card Industry (PCI) Security Standards Council. *Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures Version 2.0*. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (2010).

[Purcell 2012]
Purcell, A. *Report of the Acting General Counsel Concerning Social Media Cases* (OM 12-59). Office of the General Counsel, 2012. http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd

[Silowash 2012]
Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition* (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

[Spring 2012]
Spring, J. & Huth, C. *The Impact of Passive DNS Collection on End-User Privacy (Appendix C Section C)*. Presented at Securing and Trusting Internet Names (SATIN) 2012. Teddington, United Kingdom, March 2012. Carnegie Mellon University, 2012. http://conferences.npl.co.uk/satin/papers/satin2012-Spring.pdf

[Transparency International 2011]
Transparency International. *Corruption Perceptions Index 2011*. http://cpi.transparency.org/cpi2011/results/ (2011).

[UN 2011]
United Nations (UN) High Commissioner for Human Rights. “Discriminatory Laws and Practices and Acts of Violence Against Individuals Based on Their Sexual Orientation and Gender Identity,” *Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General, A/HRC/19/41*. United Nations, 2011.

[UN 2007]
United Nations (UN) Division for the Advancement of Women. “CEDAW: Country Reports,” *Convention on the Elimination of All Forms of Discrimination Against Women, Country Reports*. United Nations, 2007. http://www.un.org/womenwatch/daw/cedaw/reports.htm

[USG 2007]
United States Government (USG). *Code of Federal Regulations (Annual Edition) 2007. Title 45: Public Welfare. Part 164, Section 312, Technical Safeguards* (45 CFR § 164.312(2)). U.S. Government Printing Office, 2007.

[USSC 2010]
U.S. Supreme Court (USSC). *The City of Ontario v. Quon, 130 S. Ct. 2619, 2631*. Government Printing Office, 2010.

[Valdez 2009]
Valdez, F.; Buttles, P.; & Mogilensky, J. "The Role of Organizational Culture in Process Improvement." SEPG North America 2009. San Jose, CA, March 2009.

[Wikipedia 2012]
Wikipedia. *Racism*. http://en.wikipedia.org/wiki/Racism (2012).

[Wugmeister 2008]
Wugmeister, M. & Bevitt, A. *Comparing the U.S. and EU Approach to Employee Privacy*. Morrison and Foerster, 2008.
http://www.mofo.com/comparing-the-us-and-eu-approach-to-employee-privacy-02-29-2008/

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	August 2013	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Best Practices Against Insider Threats in All Nations	FA8721-05-C-0003

6. AUTHOR(S)

Lori Flynn, Carly Huth, Randy Trzeciak, Palma Buttles

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2013-TN-023

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

Based on its analysis of more than 700 case studies, the CERT® Insider Threat Center recommends 19 best practices for preventing, detecting, and responding to harm from insider threats. This technical note summarizes each practice, explains its importance, and provides an international policy perspective on the practice. Every nation can use this paper as a succinct educational guide to stopping insider threats and an exploration of international policy issues related to insider threats.

14. SUBJECT TERMS	15. NUMBER OF PAGES
insider threat, best practices, international, policies, security, information security, cultures, education	23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL