Software Engineering Institute

Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase II, Expanded Analysis and Recommendations

Lori Flynn
Greg Porter
Chas DiFatta

January 2014

TECHNICAL NOTE
CMU/SEI-2013-TN-030

CERT® Division

http://www.sei.cmu.edu

Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security 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 sponsored by the United States Department of Defense.

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

DM-0000835

Table of Contents

Acknowledgments v

Abstract vii

1 Introduction 1
- 1.1 Building on Past Research 2
- 1.2 Engaging Participants 2
- 1.3 Effort Goals 2

2 Insider Threat Vectors 4
- 2.1 Insider Threat Definition 4
- 2.2 Exposure of the CSP 4

3 CSP Responses and Related Considerations 7
- 3.1 Techniques and Controls 7
  - 3.1.1 Technical Controls to Identify Insider Threats 7
  - 3.1.2 Administrative Controls to Identify Insider Threats 9
  - 3.1.3 Physical Controls to Identify Insider Threats 9
  - 3.1.4 Mitigation Strategies to Protect Customers 9
  - 3.1.5 Awareness of Insider Risks 10
  - 3.1.6 Mobile Devices 10
  - 3.1.7 Policy and Governance 11
  - 3.1.8 Technology 12
  - 3.1.9 Outside the United States 14
  - 3.1.10 PaaS Versus SaaS Versus IaaS 15
  - 3.1.11 Requirements for Controls 15
  - 3.1.12 Highlighted or Additional CSP Concerns 16
- 3.2 Mature Processes 18
  - 3.2.1 Storage Management 18
  - 3.2.2 Virtual Machine Management 19
  - 3.2.3 Network Management 20
  - 3.2.4 Security 21
  - 3.2.5 Diagnostics 22
- 3.3 Administrative and Technical Recommendations 23
  - 3.3.1 Expand Diagnostic Sensing and Visibility 23
  - 3.3.2 Use CERT Insider Threat Assessment Workbook Capabilities for CSP SIEM Systems 25

4 Conclusions and Future Efforts 28
- 4.1 Future Research 28
- 4.2 Expanding the Relationship With and Among Cloud Service Providers 28

Bibliography 30

List of Tables

Table 1: ITA Workbook Capabilities That a SIEM System Could Use 26

Acknowledgments

This work was funded by a grant from the U.S. Department of Homeland Security (DHS) Federal Network Resilience (FNR) division. Additionally, the authors express our gratitude to the anonymous cybersecurity experts from cloud service providers who generously shared their insights and their time. Their contributions helped us better understand the controls that cloud service providers have deployed to manage insider risks as well as their concerns about their insider threat management competencies. We give a special thanks to our team member and SEI professional editor Paul Ruggiero for improvements to the report.

Abstract

Throughout the third quarter of 2013, researchers in the CERT® Insider Threat Center, part of the Carnegie Mellon Software Engineering Institute, contacted commercial and government cloud service providers (CSPs) to better understand the administrative and technical risks posed by CSP insiders and the countermeasures that CSPs are considering and deploying to identify and mitigate insider attacks. Based on the insight obtained from participating CSPs, CERT researchers have examined how existing CSP insider threat management practices may be improved. Researchers also examined the CERT Division's Insider Threat Assessment workbooks to identify some data types useful for CSP security information and event management (SIEM) systems, specifically for mitigating insider threats. A table listing those identified data sources may be of use for CSPs adding logging, analysis, and alerts to their SIEM systems. This report contains observations obtained from interview and survey responses of participating CSP personnel, considerations for improving insider threat mitigation processes, and current challenges within the CSP community as observed by the Insider Threat Center team.

1 Introduction

The year 2013 may be the year of the insider threat. Recent incidents of intellectual property theft, exfiltration of sensitive intelligence, and international espionage concerns have risen to the legal and regulatory forefront, quickly becoming a matter of political debate and public speculation. These incidents highlight the need to improve the ability of organizations to detect, deter, and respond to insider threats, which we call *insider threat process improvements*.

Successful insider attacks can have a range of debilitating impacts on the security, mission fulfillment capability, and economic viability of states and corporations, particularly of cloud service providers (CSPs). The Edward Snowden revelations that have recently captured worldwide headlines for months allege, among other things, that U.S. government agencies monitor, decrypt, analyze, and store data content and communications metadata that users send to and receive from U.S.-owned CSPs. Since these events, the Cloud Security Alliance (CSA) estimates that the major U.S. CSPs will lose $35 billion in market share as non-U.S. businesses take their data and processing elsewhere [Thibodeau 2013]; Forrester Research puts the number at $45 billion [Babcock 2013]. Media analyses have noted that non-U.S. businesses, especially in western Europe, are concerned about potential industrial espionage as well as personal privacy invasion [Abboud 2013, Samson 2013]. According to the CSA, service orders to U.S. CSPs have declined 10% since the Edward Snowden revelations were made public [Gallagher 2013].

Governments and businesses worldwide work to identify insider threats before they can endanger tangible or nontangible assets. Yet many organizations, such as commercial and government CSPs, are still coming to terms with how to identify and optimally counter the insider threat. The sheer volume and richness of their customer and corporate content makes CSPs a prime target for malicious external and internal activity, so they play a critical role in understanding and mitigating insider attacks. Details regarding current CSP insider threat management practices remain scant. Many CSPs appear unwilling to share effective practices, perhaps out of concern over competitive market dynamics or the perceived lack of an appropriate forum to securely share internal practice details.

The U.S. Department of Homeland Security Federal Network Resilience (DHS FNR) division tasked the CERT® Division of the Software Engineering Institute (SEI) at Carnegie Mellon University to analyze methods that CSPs may be using to identify and manage the risks posed by insiders. This document reports on the following outcomes of this research project:

- furthered understanding of current insider threat management practices among CSPs, obtained through interview and survey responses of three participating CSPs
- a discussion of relevant, existing insider threat best practices and controls
- an examination of CSP insider threat vectors
- an illumination of current challenges to insider threat process improvement within the CSP community

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

1.1 Building on Past Research

The current work is the second phase of a project begun in the first quarter of 2013. As a continuation of inquiry and analysis conducted in the project's first phase, researchers in the CERT Insider Threat Center contacted both commercial and government CSPs for further input on their insider threat programs.

As in the first phase of the project, CERT researchers interacted directly with CSP information security personnel via phone-based interviews and insider threat surveys. The researchers analyzed the participants' responses to identify operational processes that may be enhanced to improve insider threat management capabilities.

With new input from CSPs, research papers, and current events in cybersecurity, the current research documents more challenges specific to CSP organizations and highlights recognized practices for combatting insider activities.

The researchers also leveraged the CERT Division's Insider Threat Assessment (ITA) workbooks. Researchers examined the workbooks to identify capabilities investigated in an ITA that could be used for CSP security information and event management (SIEM) systems for insider threat mitigation.

1.2 Engaging Participants

Our goal in this phase of the project was to survey and interview multiple representatives of CSPs with large market shares. Although we made high-level contacts at large CSPs, the majority eventually declined to participate. All of them were concerned about discussing security outside of their company, and some even had policy against involvement in such a project. One specifically referenced the recent Snowden-related news stories about CSPs.

In the end, we obtained participation from one cybersecurity expert at each of three CSPs, though the companies cumulatively cover a larger CSP market share than all Phase I participants combined. We were not able to speak with multiple representatives at each CSP due to project time constraints. We interviewed and surveyed participants about cybersecurity controls at their respective organizations. This section of the report describes the information they provided, anonymized with respect to CSPs as well as to the individual experts' identities. By providing boots-on-the-ground insights about commonly implemented controls, security controls planned in the near future, and controls participants feel that the industry needs help to develop, these cybersecurity experts helped us to better understand how CSPs currently implement insider threat mitigation. Respondents did caution that some responses did not contain complete or detailed information due to security concerns.

1.3 Effort Goals

Recent CERT research on insider threat management practices at CSPs has indicated that the business processes and administrative controls that could be used to support insider threat management programs are generally unstructured and lack formal process maturity [Porter 2013]. While CSPs are certainly aware of insider risks, the safeguards that structure their insider threat management programs are primarily reactive and not institutionalized across many CSPs.

This Phase II effort aims to further expand our preliminary analysis to better understand

- if there are common threat vectors CSPs should acknowledge and look to counter when addressing the insider threat
- what techniques and controls are working well and assisting CSPs with their insider threat program
- what techniques and controls can be improved to enhance the capabilities of insider threat programs
- what insider threat processes are mature
- what administrative and technical challenges need to be addressed to help CSPs improve insider threat awareness and enhance program maturity

2 Insider Threat Vectors

2.1 Insider Threat Definition

The CERT Division's definition of a malicious insider[1] is a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

The four major classes of malicious insider threat attacks that the CERT Division has identified in its database of more than 800 insider threat cases are (1) IT sabotage, (2) intellectual property (IP) theft, (3) fraud, and (4) espionage. An additional type of insider threat could be described as abuse of power:

- insiders using, simply for curiosity or enjoyment, information the CSP client did not intend to share with those insiders [Ross 2008]
- stalking [Gorman 2013] (which, given GPS location information and email text information alone, could feasibly provide information to be used in a rape, assault, or murder)
- use of information to blackmail or embarrass others
- use of information to affect political events

The CERT Division's definition of an unintentional insider threat is a current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- through action or inaction without malicious intent,[2] unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems

2.2 Exposure of the CSP

While the CSP concept of concentrating and sharing ultra-high-density computational resources for use by multiple organizations is highly economical, that very scale and density of assets greatly increases CSPs' exposure to the insider threat. This reduces the problem set of the insider threat vector considerably by providing insiders the following advantages:

- stealth—Camouflaging and hiding within the mass of resources and processes becomes much easier, especially in high-growth, less mature CSPs.

[1] Throughout the rest of this report, the phrase *insider threat* or *insider threat vector* refers specifically to malicious insider threats, except where the full phrase *unintentional insider threat* is used.

[2] Malicious intent includes the intention to cause harm. Harm can also be caused by those who have no malicious intent (i.e., are nonmalicious), either by action or inaction, even if they knowingly break a rule (i.e., the guard who does not check badges does not mean to allow a malicious actor into the building, but she lets someone in who sets the building on fire).

- ample targets—There will always be some data asset leakage from the CSP management infrastructure as well as their customers; statistically, there is a greater chance of discovering and acquiring assets.
- complexity—The management of high-density computational infrastructures requires more expertise. A CSP's management efforts are complex, and it can be challenging to find adequate staff. These factors, plus errors in configuration, shortcuts in architecture, and implementation and operational practices accentuated by rapid growth, greatly increase the probability of opening a window of opportunity for error and, in turn, insider activity.
- time—Some CSP insiders (particularly highly privileged system administrators at the CSP or long-term contractors or business partners) have the luxury of time. They can use persistent access to implement their plan of action over a period of days, months, or even years. Preventive security measures, while instrumental in digital defense, will eventually fail. If the CSP assumes the mindset that information security breaches will inevitably occur, it can examine the ways it can detect, contain, and initiate an effective response to intrusions. CSP security professionals must layer defenses and monitoring controls such that insiders can never, ideally, completely achieve their malicious objectives.
- large threat surface—Cloud environments containing so-called Big Data represent a veritable treasure trove of attractive information for cybercriminals and are a highly desired target. Compromising elastic cloud infrastructure can return massive profits when compared to hacking into a traditional hardware-based server. For instance, if a malicious actor, external or internal, is able to place malware on a virtual machine (VM) that is later duplicated or cloned within a given cloud environment, the attacker's ability to harvest sensitive information and/or use compromised resources as desired (e.g., botnets, email/user account harvesting, extortion, denial of service) increases significantly. Beyond the implications of malicious targeting by external actors, CSPs should consider how criminals may engage internal employees as a means of gaining a prized foothold within the hosted environment (for Big Data-motivated attacks and others).

The complexity of CSP infrastructure management methods and technologies is increasing rapidly, often outpacing the process of automating the management workflow. As CSPs shepherd a given customer's assets into their environment and handle a sprawling infrastructure, a lack of adequate management practices by the customer or the CSP could introduce the following challenges:

- configuration management—Cloud elasticity is a key market differentiator for CSPs versus traditional hosting models, as virtual infrastructure can be quickly copied and migrated according to demand. However, this could increase the risk of compromise if not-hardened, vulnerable VMs are cloned across a given customer environment. As the VM is cloned, so too are any existing vulnerabilities, which could rapidly expand the CSP's threat surface for internal and external malicious actors. Additionally, preserving the state and data of a VM at a specific point in time via a snapshot may lead to a noncompliant asset (e.g., operating system/application vulnerabilities, noncompliant configuration) upon reactivation. Snapshot configuration state could increase the risk of compromise if not adequately addressed.

- compromised credentials—Depending on the VM configuration, a CSP insider may be able to obtain a memory dump, or snapshot, of the VM by using the dump-core command to access the resources (i.e., memory) reserved for the targeted VM. The resultant dump file can then be analyzed for password content. It is also possible to retrieve cryptographic keys stored in memory in a format that is recognizable, such as public-key cryptography standards (PKCS) [Rocha 2011]. This may enable the CSP insider to access customer and/or internal resources for which they are not authorized.
- information leakage—While VMs isolate operating systems (OSs) and programs from each other, the potential for side-channel attacks has been demonstrated on systems that share resources [Ristenpart 2009]. Cross-VM attacks could be launched to exploit the co-residence and engage in information leakage reconnaissance activities. The use of multi-tenancy by many CSPs means that customers' data could potentially reside on the same physical hardware as a competitor's; attacks could penetrate the isolation between VMs to compromise data confidentiality. In a cloud environment, assuming a competitor has hosted services on the CSP's platform, an insider could attempt such an attack on behalf of the competitor. Agreeing to platform isolation or disallowing multitenant hosting decreases this threat vector.
- collaboration among insider threat actors who work in different parts of a vector—If the effort is distributed into phases of reconnaissance, disruption, and control and capture, the insider may be able to more effectively evade detection, particularly when CSP insiders collaborate with customer insiders. Consider an attack that is targeting a CSP customer's assets but is stymied by the CSP's management controls, which are well protected from a CSP outsider's attack. One possible scenario could have the following workflow phases:

  1. The insiders begin to collaborate by determining how the assets and the CSP's infrastructure are managed, in order to learn the best times and methods for the attack.
  2. If needed, the collaborators execute a disruption diversion, initiated either from within or outside the CSP's control.
  3. The insider at the CSP changes the customer's configuration temporarily to allow access to the assets.
  4. The insider on the staff of the CSP customer captures the assets.
  5. The insider at the CSP changes the customer's configuration back to its normal state.
  6. The insider stops the diversion, if any.

  In this scenario, the CSP would not have any direct records of its staff accessing the customer assets. All that the records would reflect would be the insider manipulating controls during a small period of time, which the insider could have orchestrated to appear as routine maintenance.

3 CSP Responses and Related Considerations

3.1 Techniques and Controls

This section summarizes the anonymized information derived from CSPs as part of the Phase II analysis. The Phase II interview and survey responses supplement the data gathered in Phase I interviews (not included in this report).

Not all of the participating CSPs currently implement all the discussed controls, which are aggregated for anonymity. Similarly, identified concerns may not apply to all CSPs. In the following sections, due to the participants' necessarily incomplete responses, the absence of a mention of a control does not imply that the participating CSP does not use it.

3.1.1 Technical Controls to Identify Insider Threats

The participating CSPs reported using the following technical controls to identify insider threats:

- packet capture
- data loss prevention (DLP)
- SIEM systems
- intrusion detection systems (IDS)
- intrusion prevention systems (IPS)
- role-based access control (RBAC)
- configuration management systems
- multifactor authentication (MFA)
- pattern-matching single-log (non-SIEM) analysis tools
- web traffic filtering

The CERT Division's analysis included the following observations:

- Some CSPs provided high-level details regarding their SIEM system implementations. CSP SIEM systems may perform log correlation, and they may have agents deployed on endpoint systems that generate alerts reviewed in near-real time by a security team. Each alert generates a ticket documenting the investigation, including
  - router/switch configuration changes
  - password hash file modifications
  - new user additions
  - new privileged or root user permissions granted
  - novel system event, firewall event, intrusion, login, or login failure
  - password guessing
  - Secure Shell (SSH) failures (authentication password)
  - SSH invalid user
  - failed Windows logins

- Configuration management systems were mentioned as technical controls as well. One way of implementing change management controls is to query systems against an approved manifest within short periods of time. If an unapproved change is detected, the system reverts to its approved manifest. Configuration management controls can require changes to be deployed through the manifest system.
- One countermeasure is to invest in data-oriented honey pots, to attract malicious insiders to what appears to be legitimate data and fully monitor their interactions. This data may help CSPs more effectively tune their technical controls for monitoring and thwarting insider attacks.
- MFA with user groups for CSPs may involve the following: devices and systems added to groups, users added to a group based on approved access, and a hardware authentication token with a user code required. For instance, a user must have an account, be approved for access, and be a member of the network administration group to access network switches. Additionally, members of the network administration group who address network infrastructure (e.g., routers, switches, storage area networks) do not manage internal servers or workstations. An IPS/IDS is commonly used to monitor all inbound and outbound traffic, alerting the security team of any malicious code or activity. IPS/IDS alerts are then correlated and analyzed for context within the CSP's SIEM.
- One CSP participant expressed concern about current DLP challenges, for instance, determining the system's sensitivity. Large organizations often permit document sharing with external entities, but this can cause many false positive alerts, reducing the usefulness of a DLP system. In response to that concern, one suggestion for setting up DLP systems (both host and network) is to run the system in listening mode (with alarms off) for a period of one to three months to characterize normal system events and variability. Establishing such a baseline can tune the DLP system's content sensitivity so alarms truly identify unusual activity or some specified sequence of events. Creation of the baseline should include profiling of normal data (quantities, bandwidth, and file formats) sent over the network and profiling of particular types of threats to valued data. Out-of-the-box regular expressions, which drive the DLP correlation engines, often contribute to a significant number of false positives. Customizing DLP rule sets relative to a CSP's environment can be a significant resource demand, such that the true value of DLP may never be realized as the time delta between rule customization and filtering the resultant output is simply too great.
- One CSP specified that it had no formal process for monitoring social networks for ex-employees' or ex-contractors' names.
- One CSP mentioned that it does not use specific tools related to the insider threat. However, multiple tools exist within the CSP's environment that it can use to help detect, prevent, and respond to insider threat activities, for instance, using DLP to detect exfiltration by insiders. This seeming disconnect between insider threat tools being available but not being used might indicate a need for more clarity on a shared definition of the term *insider threat*, as defined in the Introduction section of this report. Additionally, tool suites that benefit an insider threat program could be organized into an insider threat taxonomy to further assist a CSP with organizing and enhancing its detective and preventive capabilities specific to insiders.

3.1.2 Administrative Controls to Identify Insider Threats

The participating CSPs reported the following administrative controls used to identify insider threats:

- pre-employment background checks, including education and criminal conviction history
- pre-access government background investigation at the minimum background investigation (MBI) level or higher
- pre-access general security-awareness training with annual recertification (includes management and executive staff)
- pre-access role-based security training with recertification every two years (includes management and executive staff)
- monthly general security-awareness sessions on current topics or threats
- separation of duties and least privilege policies—For example, engineers or administrators have access only to those systems necessary to complete their job or role. Network engineers have access only to network switches and routers. They do not have access to servers or other systems and devices. Security engineers do not have access to underlying systems or OSs.
- change management (CM) policy and supporting CM ticketing system with approval board and automatic approval assignment
- an incident response plan that covers insider threat
- exit interview and procedure to terminate access
- periodic and consistent review of access
- managers who work regularly with employees to help ensure projects are progressing and that team culture is positive
- targeted monitoring is done during a major event such as a layoff, merger, or acquisition
- a general privacy and monitoring policy that specifies the collection and retention of more than three weeks of employee online activity, which the organization can use for auditing purposes as necessary—The policy specifies that there is no assumption of privacy for employees' IT activities at work; employee agreements or logon banners are used to enforce this control. The CSPs keep large logs, and analysis includes periodic examination for leaks, activities that can result in termination, and odd behaviors.

3.1.3 Physical Controls to Identify Insider Threats

Participating CSPs reported the following physical controls used to identify insider threats:

- physical access to data centers that is limited only to those engineers with a need to access them; annual review of this access
- MFA, such as biometric palm scanners plus numeric PINs, required for physical access to the data center; person traps just beyond the CSP lobby as well as air gaps past the primary point of ingress
- security cameras in each server rack to monitor designated rackspace and equipment

3.1.4 Mitigation Strategies to Protect Customers

CSPs reported some of their strategies for mitigating insider threat and protecting customers:

- Tell insiders they are being monitored and have consented to such monitoring via logon banners and/or employee agreements.
- Maintain comprehensive access to system administrator activity, which is sent to a security organization for analysis. The reporting CSP expressed doubts about this strategy's effectiveness for detection but believed it was effective for prevention and auditing.
- Enforce RBAC. Give the right employees the right level of access for their work, and review their access levels regularly.
- Create automated or web-based tools in lieu of direct administrative access (SSH, remote desktop, etc.) to critical systems.
- Deny staff access to customer environments by default. Also deny customer access to other customers' environments or systems.
- Handle additional services for some customers through statements of work (SoWs), with the customer explicitly granting CSP staff access to any of its systems required to perform these services. Staff are subject to any additional background investigation requirements a customer may have to complete the SoW special services.
- Enforce strong education and background requirements, strict access control and monitoring, an incident response plan that covers insider threat, exit interviews and procedure to terminate access, and periodic and consistent review of access.

3.1.5 Awareness of Insider Risks

One CSP mentioned having a very small population with insider access, despite having a large user base. Having few highly privileged insiders might reduce risks as well as the number of insiders to scrutinize for insider activities. However, users of the systems and trusted business partners also have insider privileges and should be treated as potential insider threats. This is another example of needing a shared definition of the term *insider threat* (as in Section 3.1.1).

3.1.6 Mobile Devices

- The CSPs allow personal devices on-site and have formal mobile device management (MDM) policies. They permit limited use of both personally owned and organization-owned devices on the organization's network and limited organizational data on those devices.
- Mobile file management diagnostic logs are not used for insider threat monitoring. Those logs have been configured to preserve the privacy rights of mobile device users.
- One of the CSPs had a mobile device management monitoring solution, though its logs are configured to preserve the privacy rights of mobile device users. The other CSPs did not monitor mobile devices.
- One CSP enforced a policy of prohibiting personal laptops on the company network by using a network admissions control (NAC) environment in monitor mode, with the intent of locking everything the CSP does not recognize.

One CSP expressed concern about the difficulty of enforcing limited use of personal devices on the organization's network. Technical controls that could help include

- USB port monitoring

- controls limiting network and machine port connections to whitelisted Media Access Control (MAC) addresses
- network scanning to identify and reject machine profiles (beyond MAC addresses) that are not on a whitelist
- NAC in monitor mode

Future research could investigate integrating mobile device and/or MDM data into CSP SIEM platforms for correlation and analysis, as well as using such data to assist with insider threat detection, particularly exfiltration of sensitive information.

3.1.7 Policy and Governance

3.1.7.1 Governance

Governance measures included conformance to specified best practice standards (sometimes but not always including certifications), incident response programs, and specific insider threat programs. Some of the specified best practice standards include ISO/IEC 27001:2005 [ISO/IEC 2005] and the Federal Risk and Authorization Management Program (FedRAMP).

Although one CSP mentioned having an insider threat program, the others did not. The CERT Division's *Common Sense Guide to Mitigating Insider Threats, 4th Edition*, describes how to create an insider threat program in its chapter on Best Practice 16, "Develop a formalized insider threat program" [Silowash 2012]. It states that an effective insider threat program requires setup ahead of an insider threat incident, and it must include high-level representatives of the CEO, CIO, CISO, CFO, COO, and chief legal counsel, if not the officers themselves. To most effectively mitigate insider threats, specific types of controls (administrative, technical, and physical) must be put in place.

Companies may find it hard to justify spending money to start an insider threat program to those who make investment choices within the company, particularly if the financial risks of *not* having an insider threat program are not quantified. For example, one CSP mentioned its extremely successful employee training against phishing attacks, with easily measurable success metrics and relatively low cost. Anti-phishing training, which works to reduce *unintentional* insider threats, raises employees' awareness and caution regarding warning signs in malicious emails and websites that contain links or viruses. The CSP noted that it was difficult to compare the return on investment (ROI) between investing in running an anti-phishing training program, versus investing in security measures to mitigate threats from malicious insiders. (Measurement on subsequent tests showed impressive results: a 40% decrease in clicking on a link after the training and a 100% improvement in not executing malicious code.) Though federal agencies and departments that handle classified data have been required to stand up insider threat programs [Obama 2012], non-government CSPs do not currently have that requirement.

CSPs also mentioned their always-available (24/7) incident response teams. These teams could respond to insider incidents as well, though some concerns about this particular capability were noted.

3.1.7.2 Background Checks

The CSPs perform background checks before hiring, but not always after hire. For particular work tasks, pre-access government background investigation is required at the MBI level or higher as a requirement and condition of employment. Beyond that, DoD clearances are required for particular positions.

One CSP's perception was that some workers outside the United States can perceive a background check as a sign of not being trusted as a foreigner. This highlights the importance of clear communication about the nondiscriminatory nature and consistent application of background check requirements.

The CSPs did not mention periodic re-investigations at regular intervals after hire, beyond DoD re-clearances. If a CSP's relevant (and legal) background checks might change over time, then we recommend regular re-investigations. Additionally, as the degree of the insider's access increases, the depth of background checks should increase proportionally, though always in accordance with the law.

One area of related research involves combining background information or psychological profiling metrics with network-based data, such as anomalous network activity, to detect at-risk employee behaviors. We have not been able to find statistically significant research results comparing network-based data of normal populations to network data of insider threat attackers or, similarly, comparing psychological profiling metrics or background information of a base-case population to an insider-threat-vector-only population. This is an area of active research [Moore 2009, 2012; Mundie 2012] whose future findings may inform background checks.

3.1.7.3 Third-Party Contractors

On-boarding and monitoring of third-party contractors or vendors within the organization's IT environment can be a challenge, though our observations during this study suggest that contractors are rarely used in the security domain, especially in the highest privilege domains.

One control is an access enforcement policy that denies a contractor's access until the contractor goes through a standard on-boarding process and comes under the CSP's central oversight. That same central oversight is used to close out contractor work at the CSP through an off-boarding process, assuring timely tracking of a contractor's departure. This control allows the CSP to immediately terminate the contractor's accounts and accesses when the contractor departs instead of when, for example, the contract ends, by which time the contractor may have already departed.

3.1.8 Technology

3.1.8.1 Management and Visibility

Some of the techniques used by CSPs for management and visibility into possible technology misuse by insiders include the following:

- Monitor the control planes of their infrastructure for staff's abnormal behavior that may indicate an insider incident.
- Isolate diagnostic logs and restrict their access by staff on a need-to-know basis.

- Implement separation of duties, in which multiple individuals and keys are required for sensitive operations. To perform those operations abusively or as part of an attack, malicious insiders would need to collude.
- Use a tool to enforce and monitor administrative privileges.

The following are some suggestions for management and visibility controls that were not mentioned by the CSPs:[3]

- Use custom rule sets for SIEM technologies to monitor the control planes of CSP infrastructure (e.g., network, infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)) for staff's abnormal behavior that may indicate an insider incident. As mentioned above, combining SIEM data with user profiling metrics could significantly enhance the CSP's ability to identify insider threats.
- Isolate diagnostic data repositories (logs) and restrict their access by staff on a need-to-know basis.

3.1.8.2 Virtual Machine Environment

To address insider threats in the VM environment, CSPs

- closely monitor version control and signatures on images, as well as any software that may be included within them that a customer would use
- securely delete memory prior to its initial assignment to a specific VM
- ensure VM diagnostic tools do not expose the details of hypervisor events to staff, which could compromise the customer's security

One control suggestion not mentioned in the participants' responses was to closely monitor and audit the control plane of the VM infrastructure for abnormal behavior by internal staff.

A vital step toward securing CSP infrastructure is to ensure that firmware, OSs, and applications are sufficiently patched and hardened against attack. Maintaining attack-resistant software configurations makes it more difficult for intruders to gain a foothold. A continuous monitoring program should monitor configuration settings, system files, running processes, ownership, and permissions to ensure that no unauthorized changes are made. The National Institute of Standards and Technology (NIST) provides useful guidance for federal information systems and organizations [NIST 2011].

There is an important distinction between continuous monitoring and network security monitoring (NSM). Some might assume that if an organization practices continuous monitoring, then NSM is unnecessary. Unfortunately, continuous monitoring has almost nothing to do with NSM, or even with trying to detect and respond to cyber-related incidents. As described by Richard Bejtlich,

> *NSM is threat-centric, meaning adversaries are the focus of the NSM operation. Continuous monitoring is vulnerability-centric, focusing on configuration and software weaknesses. For continuous monitoring advocates, "continuous" means checking system configurations more often, usually at least monthly, which is a vast improvement over previous approaches. The "monitoring" part means determining whether systems are compliant with controls—that is,*

[3] As stated earlier, a CSP's failure to mention a control does not indicate that the CSP does not implement it. Participants explicitly stated that they intentionally withheld some information on their cybersecurity controls.

determining how much a system deviates from the standard. While these are laudable goals, continuous monitoring should be seen as a complement to NSM, not a substitute for or a variant of NSM. Continuous monitoring can help you to provide better digital defense, but it is by no means sufficient. A continuous monitoring operation strives to find an organization's computers, identify vulnerabilities, and patch those holes, if possible. An NSM operation is designed to detect adversaries, respond to their activities, and contain them before they can accomplish their mission. [Bejtlich 2013]

Both continuous monitoring and NSM are essential practices when defending against the insider threat.

3.1.8.3 Data Storage

CSPs mentioned the following controls used for securing data storage:[4]

- One policy requires customers to encrypt their own data when it is stored on the CSP's systems, also leaving management of encryption keys to the customers. Another customer-based control gives the customer discretion to decide if and how to handle archive storage.
- Retired disk drives are degaussed or destroyed prior to removal from the premises.
- Hard copies and digital media containing sensitive information are shredded as part of disposal processes.
- The lifecycle of diagnostic data (e.g., event logs) is governed by policy.
- Data deletion follows industry standards for physical data destruction, with all virtual storage scrubbed, whether customers delete their own services or the CSP deletes them as part of a decommissioning process.
- The CSP maintains no rights to customer data once a contract is severed.

Secure and complete deletion controls are advised.

3.1.9 Outside the United States

Effective implementation of cybersecurity best practices may require varying types of controls (technical, administrative, and physical) in different countries, particularly depending on five factors: laws, law enforcement, corruption, IT systems, and culture and subcultures [Flynn 2013].[5] CSPs mentioned the following considerations:

- One CSP said that it follows industry standards for data storage, regardless of location, whether in a developed or developing country.
- The CSPs are forced to change some physical, technical, and administrative controls for facilities based outside the United States.
- In developing countries, some controls, such as prohibiting mobile phones and cameras at work, can be imposed that cannot be imposed in more developed countries such as the United States.

---

[4] See Section 3.1.9 for discussion of data storage outside the United States.

[5] Flynn, Lori; Huth, Carly; Buttles-Valdez, Palma; Theis, Michael; Silowash, George; Cassidy, Tracy; Wright, Travis; & Trzeciak, Randall. *International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany* (Technical Report). Software Engineering Institute, Carnegie Mellon University, pending.

- One type of control being used in developing countries includes limiting the local ability to do things that have a broad impact. This includes not allowing CSPs to set up their firewalls locally or control their servers' configurations locally.
- By signing on to the U.S.–E.U. Safe Harbor Framework (or the U.S.–Swiss Safe Harbor Framework) [Department of Commerce 2012], CSPs for European Union countries with high privacy requirements could manage data storage and services largely uniformly.

Participating CSPs wanted more information about suggested controls for developing countries. The CERT Insider Threat Center is currently revisiting some of the controls used in developing countries, with consideration of ways to lower risk exposure and strengthen the controls. Broadly speaking, developing countries do not support different types of controls (i.e., physical, technical, and administrative). Periodic audits of CSPs in developing countries have found sloppiness and weakness in the implementation of controls, whether actual or claimed on paper by the provider, and some actual implementations have been found to be weaker than claimed. Cultural barriers to communication and implementation of policies are a concerning issue. Some guidance can be found in the CERT Division's international cybersecurity best practice analysis framework, first described by Flynn [Flynn 2013] and as applied to India and Germany.[6]

3.1.10 PaaS Versus SaaS Versus IaaS

One CSP commented on insider threat differences between PaaS, SaaS, and IaaS providers. Customers utilizing a PaaS or SaaS solution make it easier for insiders to see data within their applications. IaaS puts a larger divide between employees and customer data because the data is held in a VM. Access to all of these systems is strictly controlled, but there is additional monitoring on PaaS products for malicious activity, due to the nature of the product.

3.1.11 Requirements for Controls

When we asked the CSPs about what kind of insider threat controls would be useful to them (even if the controls do not exist yet), they replied as follows:

- information on the utility of different types of data on workforce members, to indicate if someone might be an insider threat[7]
- more information about how to usefully monitor highly privileged users
- quality of data (raw and intermediate)
- verification and role-based access
- semi-automated way to identify behaviors and isolate deviations to be investigated by a team of individuals—Triggers would be based on possible behaviors correlated to exfiltration and on integration of some system dynamics modeling.[8]
- more statistical tools

---

[6] Flynn, Lori; Huth, Carly; Buttles-Valdez, Palma; Theis, Michael; Silowash, George; Cassidy, Tracy; Wright, Travis; & Trzeciak, Randall. *International Implementation of Best Practices for Mitigating Insider Threat: Analyses for India and Germany* (Technical Report). Software Engineering Institute, Carnegie Mellon University, pending.

[7] As noted earlier, this is an area of current research.

[8] Though these are topics of research, definitive correlations between behaviors and insider threats may not currently exist.

- more assistance with insider threats arising from bring-your-own-device (BYOD) policies

3.1.12 Highlighted or Additional CSP Concerns

The CSPs shared issues of concern regarding threats from trusted insiders:

Insufficient Data-Gathering Capabilities

- Most of the detection capabilities to gather evidence are insufficient. They may provide forensic data but not alert triggering mechanisms. There is not much perceived capability for detecting insider threat.
- More information is needed on USB-drive usage events, such as insertion, copies to or from the device, and removal of the device.

Inadequate Statistical Analysis

- Though CSPs have some capability for semi-automated statistical analysis based on behaviors, they do not know what behaviors to look for. CSPs also expressed that there is a lack of effective rule sets and signatures for detecting insider behaviors, for instance, signatures that can be implemented within IDS/IPS, SIEM systems, or both. The CERT Division has previously described the development and proposed application of a SIEM signature to detect possible malicious insider activity leading to IT sabotage [CERT Insider Threat Center 2011], and this is an area that warrants future research considerations.
- More statistical tools are needed to better identify potential insider threats and attacks.
- RBAC is imperfect, and it should be statistically examined. Aspects of interest include the typical response time for account activation and deactivation following a new hire or termination, the type of metrics that typically result when enterprise analyses are performed for rogue accounts, and similarly the type of accounts that are typically over-privileged and how that is effectively monitored and tracked.

Particular Insider Threat Models of Concern

- Most CSPs follow basic access management principles regarding the need to know, but insiders still have a huge amount of access.
- One of the insider threat models of concern is a nation-state model. After examining data exfiltration per country, there are concerns about specific countries possibly attempting to target and enter companies in sensitive roles, for the sole purpose of extracting information.
- Major staff events such as a reduction in force (e.g., layoffs) are an area of concern. CSPs might consider working with an external organization that looks for employees who may be negatively impacting the workforce and works to positively and securely handle such employees.
- Whistleblower syndrome is a concern. One CSP respondent suggested that it comes down to leadership and company culture, and that it is very important to create a trusting, ethical culture aligned with communication. The CSP respondent thought that may prove more useful than investing in reactive methods or in monitoring that might not be ethical.
- Techniques such as examining payload, both per flow and in packets, and performing monitoring at the network layer, are rightfully perceived as facilitating the prevention, detection, and response to some insider threat incidents. However, there is a concern that savvy insiders (highly technical and, perhaps, sponsored by states or large crime

organizations) tend to have more training to combat such detection methodologies and so are less likely to use commonly known exfiltration techniques. There is also a desire to understand more about the techniques those savvy insider threat vectors are using. This is yet another area that warrants further examination and research.

Questionable Return on Investment in Some Controls

- Risk assessment frameworks present their own challenges. For instance, the organization could spend too much time analyzing the problem instead of correcting it. CSPs are also concerned about the amount of time invested in risk management frameworks versus improved outcomes.
- Employees might feel untrusted and spied on in a way that would have negative effects on teamwork, creativity, and performance. Culturally, CSPs have to balance between not creating a surveillance state and attracting and maintaining talent, so they need to maintain a degree of openness and an environment that people want to come to.
- Attempts to associate ROI with security controls might be impossible to do accurately or usefully.

Inadequate Guidance About How to Mitigate Insider Threats

- There is not sufficient guidance, particularly legal guidance, about how to set up and run an insider threat program. Most CSPs would like to learn more about building an insider threat program and sharing information from various departments in some kind of trusted group, considering legal, ethical, and effectiveness concerns simultaneously.[9]
- Scientific, relevant guidance is needed to guide the development of attribute profiles, background checks, technical indicators, and a taxonomy of insider threat actors and their motivations (e.g., criminal, political, ideals).
- Guidance is needed about how to decompose indicators in order to prioritize investment in security controls against insider threats.
- Legal concerns prevent CSPs from sharing information between Human Resources (HR) departments and managers of different groups—communications that could alert these groups to possible problem staff members.
- More information is needed on how insider threat actors behave, that the CSPs could use to better prevent, detect, and effectively respond to insider threats.

Ineffective Security Training

- It is difficult to change human behaviors, ignorance, and behavioral challenges that have associated vulnerabilities with respect to social engineering through emails and phone calls, habits of politeness and door-holding that weaken security at doors, insecure care of electronic badges, inattention to badges with clearly different photos than the badge carrier, and other manipulations.
- There is a need to focus on what makes training effective. For instance, group conversations within teams greatly reduce user errors within the group. What other methods could improve training effectiveness?

---

[9] See the CERT Division's *Common Sense Guide to Mitigating Insider Threats, 4th Edition*, Practice 16, "Develop a formalized insider threat program" [Silowash 2012].

3.2 Mature Processes

We observed that a number of CSPs have a set of practices, processes, and methodologies to guard against the insider threat vector. The following are notes based on CSP survey and interview responses,[10] supplemented with relevant good practice information for mature processes and with data source information for SIEM systems.

3.2.1 Storage Management

Storage management services, both for customers and internal to the CSP, are one of the primary targets of the insider threat vector. The data has intrinsic first-order value, but it can also provide a wealth of second-order information: analyzed data can be used to infer information through data correlation techniques. For instance, some CSPs have adopted a data-asset-centric security methodology that assigns the data a value-based metric that defines its importance and helps determine adequate investment of resources to protect it. The metrics are usually based on some combination of accessibility, availability, confidentiality, integrity, retention, and other attributes.

During all lifecycle phases of data storage management, mitigating the insider threat vector requires CSP controls. During the initial request for storage resources, the CSP must ensure that newly instantiated resources retain no evidence of past data. CSPs sometimes use block-level devices that scour blocks of any data remnant prior to their allocation to a customer. If file system services are offered, they must be tightly provisioned to separate customers from each other as well from the CSP staff. Most CSPs make a point within the customer's service-level agreement (SLA) that protecting data is the customers' responsibility, and it is up to them to manage it by encrypting the storage allocated at a block level, the file system, or individual files, any of which includes managing the encryption layering, associated keys, and credentials.[11] When the customer returns the storage resource, the CSP must de-allocate it, scour it again, and return it to the available block pool.

Even with mature scouring methods and techniques, migration of data among active blocks may still leave remnants. The problem is amplified in the highly redundant block storage devices and appliances, not to mention off-premise storage (outside of the data center), that CSPs need in order to ensure high-availability services. We have observed a number of scenarios in which a customer leaves a CSP's IaaS, PaaS, or SaaS, but its data remains online for some time; in some cases there may be no clear policy for its removal unless it is explicitly stated within the SLA. In the best case, depending on the encryption strength and the amount of computing effort it would take to stitch relevant blocks into a set where the data could be extracted, it would take substantial effort for the insider threat vector to gain access to the data, but it is still possible. On the other hand, if the storage service had only light encryption or if the storage is application based (SaaS), it would be much easier for the insider threat vector to gain access. In this scenario, the protection would then be the responsibility of the CSP application or its back-end storage resources (such as a database) to ensure adequate protection of data. Given these scenarios, the transition of customer applications to terminate contracts, migrate platforms, and/or upgrade services should

[10] These processes are not common to all CSPs.

[11] While there have been rumors that some CSPs are offering storage encryption services to their customers, we have not encountered such a service during our study. It is unclear how the key and credential management as well as the control of this service would be provisioned to guard against the insider threat vector within the CSP.

include a security assessment detailing the impact of the transition and accounting for the potential of information leakage at both the hardware and software layers.

The control plane is probably the most critical point within the CSP infrastructure for insider threat protection with respect to storage services. The control planes of the block-level devices and appliances, as well as the provisioning framework, are all susceptible. While we did observe that many CSPs had different granular approaches, the most common techniques to guard against the insider threat were the following:

- use of a high-level user interface (UI) that allows customer managers to allocate and resolve storage problems, restricts the customer managers' use of storage service primitives, and logs activity
- at a system and device level, restricting and provisioning CSP storage teams to a select few that have different roles, such as to
  - focus on diagnostic tasks that have no direct control of the service primitives
  - control the service primitives but highly monitor them, in some cases with both the internal group and an external security group

The diagnostic data (e.g., logs, system and network events) is invaluable in solving problems, ensuring cloud health, and providing information that helps to evolve the service. However, depending on its degree of granularity, diagnostic data is a source of high-value information for the insider threat vector. It provides a detailed view of the landscape of critical storage infrastructure components, their behavior, and the CSP customers' use. Access to this diagnostic data should be highly restricted, aggregated, or anonymized.

3.2.2 Virtual Machine Management

During the past decade, virtualization has been the primary way of transforming traditional hosting organizations into CSPs. Its maturation has spawned the IaaS, PaaS, and SaaS frameworks that CSPs have used to build successful service offerings. VM management methods and technologies have spawned various new products as well as business models, but their use has brought issues of management complexity that could, if unchecked, provide a large opportunity for the insider threat vector.

VM platform feature sets have advanced greatly in the past five years, particularity in near-real time transfer of running VMs across hardware platforms as well as the ability to capture diagnostic events not only within the hypervisor but also at more granular levels such as at individual VMs. These two features alone could almost give an insider carte blanche access to CSP customer information.

Use of a VM framework exposes customer vulnerabilities by allowing key CSP personnel to observe traditional OS processes. For example, because the hypervisor manages VMs at a low level,[12] a system administrator can take a snapshot of a host, making it possible to examine data at an intruder's leisure; the data might have been encrypted within the storage or network services, but it is now exposed as a live process in memory. The control that VM management consoles present to system administrators by exposing hypervisor primitives is unprecedented. Also,

[12] Hypervisor low-level management includes controlling and scheduling VM access to the CPU and memory.

hypervisor diagnostic functions and event monitoring can be used to gain a detailed view of the landscape of the IaaS, PaaS, and SaaS customer configurations and operational behavior. As mentioned previously, reactivating a snapshot could give rise to other issues related to configuration management, such as re-introducing a system that is out of compliance with the current patch cycle and thus vulnerable.

The key to protecting both the CSP's internal assets and customers' assets lies with the control plane of the VM hypervisor. CSP practices tightly control access to the VM control consoles and use role-based functionality to restrict what staff can do. Also, many levels of the VM infrastructure should be monitored and correlated with other diagnostic domains, such as the network and security tools that monitor internal management events for suspicious behavior.

Most large CSPs have built internal monitoring systems that focus on operational domains including VM management. But given the rapid growth of CSPs, most of their systems have evolved in a nonstructured way, usually spurred by a past security event or rapid customer acquisition. Large CSPs can afford to build robust, customized, security-hardened, highly detailed VM management infrastructures because they have the right resources, such as mature development teams. Smaller CSPs do not have this luxury, and though they do try to limit the access of their staff, their resource limitations may expose them to security blind spots. Vendors of VM management infrastructures could fill this gap, but given the expense of such infrastructures and the pressure for CSPs to be profitable by cutting operational costs, there is a movement to more cost-effective, open source offerings; filling this gap may take time. Unfortunately, the open source security solutions usually lack features found in commercial solutions or ones that larger CSPs have developed in-house.

3.2.3 Network Management

CSPs have traditionally devoted generous resources to internal network security, not only because of its inherent role as the central nervous system of their infrastructures, but also because initially the technology was one of the only domains where some management centralization could occur.

CSPs' own internal networks expose them to the insider threat vector. For example, vulnerabilities could exist in the routing infrastructure or in packet capturing at the edge, resulting in internal denial of service (DoS) and/or data exfiltration of CSP and customers assets. Large-scale network configuration infrastructure products have been mature for more than a decade. Some products have feature sets that would monitor the control plane in such detail that they would capture the key strokes of a system administrator to check for validity, send them to diagnostic repositories for analysis, and then alert team members for both valid and invalid use. Network management is likely an area that has the most mature methods, products, and tools to guard against the insider threat vector.

The main network management issue facing CSPs at this time appears to be complexity and scale, as well as the discipline to impose standards for guarding against the insider threat vector. Large CSPs offering all types of services (IaaS, PaaS, and SaaS) have a good handle on the problem. They understand how to provision network micro-services and functions into specialized vertical teams, not necessarily because of design but because of scale, and so have made segmentation much easier. The scale issue also translates to horizontal segmentation: consider a large CSP that

has multiple teams located in different places managing the internal routing infrastructure that allows the teams to monitor and verify each other's security assurance functions.

At a basic level, effectively addressing the insider threat vector in the network domain (as with others) comes down to the resources and maturity of the CSP.

3.2.4 Security

Traditional data center security has long relied on layered controls to defend the hosted infrastructure from malicious external and internal attacks. Network demarcation zones (DMZs), firewalls, IPSs, and, more recently, SIEM technologies offer the ability to inspect all ingress and egress network traffic for suspicious content. However, in today's cloud models, customer data resides on a server physically controlled and managed by the CSP, and a given CSP environment may or may not offer the degree of granular network topology control necessary for optimized network security monitoring. Modern SIEM solutions are capable of analyzing and correlating syslog data from any number of devices, ranging from client workstations and servers to routers, firewalls, IPSs, and other unified threat management platforms. Yet foundational elements, such as control of IP addressing, physical topology, and routing, may be handled strictly by the CSP with little input afforded to customers. For instance, shared CSP hardware infrastructure can make obtaining specific flow data from a switch or router difficult to obtain, because flows for multiple hosted customers may be present on a single switch or router instance and would thus have to be filtered before being provided to the customer. This takes time and money and may require an upgraded cloud platform with dedicated hardware and physical separation. Additionally, many CSPs segment layer-three traffic at the VM level, so a VM can view only its own traffic, rendering network security technologies such as IPS and SIEM less effective and creating an opportunity for insider attacks.

Cloud computing is not intrinsically more secure than other distributed computing approaches, but its scale and uniformity facilitate and enable the wholesale and consistent application of security practices. Secure aspects include large-scale monitoring and analysis of data to detect attacks as well as automated and persistent provisioning and reprovisioning to foil intrusions. For these reasons, well-operated cloud computing facilities can exhibit better security hygiene than conventional data centers. However, the centralization of resources in a huge data center also encourages more determined attacks, especially on critical components broadly affecting security. This is similar to conventional systems, where attacks focus on central directories [Department of Defense 2013].

Offensive security exercises within the CSP, such as red teaming, can identify the existence of vulnerabilities that may have arisen due to poor internal configuration management or customer hosting processes that are beyond the immediate control of the CSP, for instance, through an SLA. In the absence of actually testing systems for expected security and compliance measures, there is no way to validate what is a material security risk to the business and what is not. Cloud elasticity means that a software- or hardware-based vulnerability, left unaddressed, could propagate rapidly. Red teaming can identify such weaknesses and should be performed on a defined, well-managed basis. While CSPs participating in this study do perform offensive security testing when necessary, these processes could benefit from correlation to understood insider threat vectors.

When developing security controls within the context of a cloud-based environment, a CSP must establish a disciplined and structured process that integrates information security and risk management activities into governance processes. While the CSPs that participated in this research appear to follow documented and implemented risk assessment practices, the enterprise risk assessments can be improved to focus on insiders as a potential threat to the confidentiality, integrity, and availability of the CSPs' mission-critical information. Of particular importance are technical controls that can help identify the insider before his or her goal is achieved. To this end, network security monitoring is an invaluable component for detecting insider activities.

Ensuring that appropriate hardware and software resources are available (and isolated if necessary) prior to implementation will provide the ability to monitor virtual resources and security-based cloud operations and events, as well as to generate reports that include relevant performance measures and potential indicators of insider threat activity.

3.2.5 Diagnostics

In the past decade, many disciplines, domains, and methodologies have focused on gathering reconnaissance and providing visibility into anomalies in service (e.g., disruption), SLA and operational-level agreement (OLA) conformance, and policy (i.e., violation). Diagnostics has been a grass-roots effort in specific domains such as networking, service management, middleware, storage, and security, to name a few. The past five years have seen progress in combining the diagnostic capabilities of many domains, as well as their ability to share information to greatly enhance their information and knowledge about the event horizon of their cloud infrastructures.

In general, most domains (such as networking) manage their diagnostic infrastructures (DI), where their data is very specific to their discipline. There has been a movement to combine different diagnostic data types, which greatly enhances the visibility of anomalies and the accuracy of the diagnosis and decreases the time needed to identify the root cause. Information event management (IEM) technologies have been maturing for quite some time. IEMs began in the security domain with SIEM, but they are rapidly moving to other domains to orchestrate the consumption, correlation, and analysis of events and expose key indicators to analysts.

Traditionally, CSPs have had the resources to employ experienced development teams that built IEMs and analytics for their specific domains. Early on, CSPs learned how to address issues of scale and the rapidly changing landscape of problem identification and mitigation by providing both general and specific analytic tools as well as the frameworks to build them. Because of their basic business needs, CSPs have been at the forefront of multidomain event orchestration that feeds diagnostic infrastructures. With respect to the focus of this research, most CSPs have mature security diagnostic infrastructures and processes, but in general they are focused on the external threat and are just beginning to become aware of the threat from within.

Mature CSPs use DIs to ensure security requirements, operational policy of the data assets, and the infrastructure that manages them. Control plane auditing uses the DI to monitor, audit, and verify the employee's use of command primitives for the operations and management of specific service infrastructures. Examples of control plane services that are audited across a CSP using the DI include, among others,

- configuration management (e.g., IaaS, PaaS, SaaS)

- monitoring of services (availability, performance, compliance, etc.) and access to the DI
- patch management (supporting infrastructure, images, etc.)
- content and storage management

Some CSPs are developing insider threat assessment (ITA) teams that use the CSP's DI extensively as an event orchestration platform to bring information to the analyst, who can build specific automated and forensic tools to look for anomalies that could be potential key indicators. The practice of having an ITA team using the DI is not widespread across all CSPs. It has been observed mostly in more experienced organizations. Section 3.3.2 provides suggestions about how a mature system with a SIEM could integrate various data sources useful for mitigating insider threats.

3.3 Administrative and Technical Recommendations

3.3.1 Expand Diagnostic Sensing and Visibility

While the possibility of using the DI of the CSP as an analysis platform for addressing the insider threat is extremely promising, it is not without challenges. In large CSPs, obstacles include the scale of transactions, variances of processes within CSP operational teams, lack of standards (log formats, etc.), integration with authentication/authorization services, and integration or federation of multiple DI administrative domains to correlate events. While these challenges may seem daunting for both the DI and ITA teams, the initial work on expanding diagnostic sensing should adopt an asset-centric security methodology, to identify and prioritize what parts of the organization are most susceptible to the insider threat. The following are some suggested areas for improvement where leveraging diagnostics can give an advantage.

- control plane use profiling—Increased monitoring of the control planes is highly warranted, and profiling normal activity will help identify anomalies that can indicate a possible threat and dictate additional analysis. Also, CSPs should involve the internal team that owns the specific control plane in question. Consider using feedback from managers to verify activity and to reduce false positives.
- mapping insider threat metrics—Consider compiling highly specified metrics that are easily collected and maintained and that can be manufactured from different types of data. Include sets of common and specialized indicators based on the responsibility and charter of the internal team to be monitored. Map metrics to events within the DI so that their collection and correlation can be highly automated and easily expanded.
- monitoring the incident response (IR) process—IR teams could have an unprecedented view into vulnerabilities and threats as well as into the workflow of an intruder. However, the IR teams' self-perception of being part of the organization's security apparatus could blind the team to the insider threat risk posed by its own members. The IR team's access to critical information, as well as their communications within and external to the CSP, should be monitored and restricted. When the CSP is servicing high-profile customers with sensitive data, consider restricting the IR team's use of smartphones and devices and forcing communication over traditional telephony technologies where call records can be obtained. If the organization uses voice over internet protocol (VoIP), the DI could consume call records. When working in areas with sensitive data, use dual-control mechanisms, in which two

employees must take action prior to any high-risk IR workflow, to control and confirm that the task adheres to operational policy.

- including HR information—Collect and expose HR metrics and import them into the DI, in accordance with legal guidance about what data, if any, can be imported. Use scientifically significant findings about which HR data are relevant. Use techniques, similar to those in other domains, that indicate that the level of monitoring of an individual should be elevated. Build visual interfaces that have functionality allowing a manager to increase the level of monitoring of an employee. Consider using a set of rules that can be applied to the visual interface to generate a heat map application to indicate possible suspicious indicators, which could then enable drilling down into additional forensics.
- insider threat warehouse—The DI is mostly made up of four major component layers: sensors (system events, logs, network events, etc.), data orchestration framework, middleware pre-analysis, and post-analysis tools. At the middleware pre-analysis component layer, an organization could build a warehouse that acts as a repository for first- and second-order diagnostic indicators for defined insider threat metrics. One of the primary functions of the warehouse would be to build a behavioral (IT behaviors, possibly more) repository for high-risk employees depending on their responsibility and access for managing key CSP and customer assets.
- nontraditional data sources—Incorporate new types of data sources, such as wireless activity (cam tables or wireless controller logs) and physical access records from environmental controls (door access), into the DI to indicate the possible physical locale of the user in question.

It is extremely attractive to have access to a large DI and the resources to apply insider threat efforts to the wealth of information that it affords. Unless there is a plan that builds on iterative improvements scoped for success, it may be quite some time before the investment is effective. The following are suggestions for the CSP insider threat team on how to increase the diagnostic sensing and visibility by building from the existing DI:

- Adopt and promote an asset-centric security methodology that can define insider threat metrics.
- Scope the initial effort for success, and choose an insider improvement effort targeted at a part of the organization that is high risk and can best represent other efforts that are later in the improvement queue. Target the first few efforts as a discovery effort to learn development and implementation practices using the DI.
- Use existing technologies and methodologies of the DI where possible.
- Build from the perspective of the insider threat analyst as well as the staff who will be in the workflow, generally within the group being monitored (such as managers). Gather requirements as if resources were unlimited, then scale back appropriately to the available resources, but consider the most important features for the analyst. Compile a list of questions (in analyst-speak) that analysts want answered. Constantly solicit feedback from the target users when functional tool milestones are met. Mock up UIs, make them as functional as possible, and involve the end user in their design.

- Focus on tools that are highly configurable by the end user and that create new data sets that can be consumed by other tools.
- Examine the operational standards of the team that architects, develops, deploys, and maintains the DI and, where practical, gauge their effectiveness against recognized codes of practice.
- Consider building alerting and reporting applications that leverage the DI's information sets.

3.3.2 Use CERT Insider Threat Assessment Workbook Capabilities for CSP SIEM Systems

The CERT Division's Insider Threat Assessment (ITA) examines an organization for a battery of controls (technical, administrative, and physical) against insider threats, as well as relevant documentation of policies, availability of policies for reference, and training on policies. Teams use ITA workbooks to guide the examination and note the information found. All information gathered by an ITA is relevant to insider threat mitigation. We examined the ITA workbooks with the goal of identifying data that could be used with CSP SIEM systems for insider threat mitigation.

There are seven ITA workbooks, covering the following domains: human resources, IT, legal, physical security, software engineering, trusted business partners, and data owners. We found information that could be used in a SIEM system in all the workbooks except for the one focused on legal issues. Of all the workbooks, the IT workbook identified the most information fields that could be used by a SIEM system. Information fields are identified as top-level capabilities, with more granular, lower-level indicators within those fields. A total of 40 top-level capabilities were identified that could be used with CSP SIEM systems. Many top-level capabilities had multiple lower-level indicators that could be used with SIEM systems. Table 1 lists the workbook identification code, or *capability sequence*, and describes the associated data that could go to a CSP SIEM system for logging, analysis, and alerts. Note that most CSPs have diagnostic infrastructures that encompass the SIEM, whose capability varies greatly. The following table suggests only at a high level some of the desired event streams that the SIEM could consume to begin to warehouse relevant information from potential insider threat actors. The CERT Division's ITA workbooks contain more information about potential sources for each of these data streams.

Table 1: ITA Workbook Capabilities That a SIEM System Could Use

Capability sequence	Data that goes to SIEM system for logging, analysis, and alerts
D02.2	use of an exception dashboard by system administrators at the CSP—The messages should contain enough information to allow the organization to monitor for improper usage of the exception screen.
D02.3	exception handling (system unavailability, supervisor overrides, etc.) processes
D02.4	attempts to delete types of sensitive data that could cause a DoS—Components covered should include virtual machines, processes, and stored data, including customer, payment, or billing information. Because virtual machines, processes, and stored data may sometimes need to be deleted for valid reasons, a subset of this information might be logged to SIEM systems.
D03.1	employee attempts to exceed authorized access to systems or applications controlled by data owners
D03.2	employee activity inconsistent with job responsibilities
D03.3	detection of any of the following: • downloads of confidential information outside employees' domains of responsibility or within their domains of responsibility but involving a greater quantity of information than usual • downloads close to the date of employees' termination (within 30 days before) • large downloads over short periods of time • downloads before or after normal working hours • downloads of employee or customer lists and personal information • downloads of materials shared with business partners • downloads of materials targeted for disposal • downloads of intellectual property (IP): strategic plans, source code, scientific designs and formulas, and merger and acquisition plans
HR1.11	behaviors monitored for • involvement with the internet underground • fraud • information/privacy violations • timecard and other financial reporting • information theft
HR1.17	personnel activities on the organization's proprietary IT and communications systems
HR1.17	targeted monitoring
HR1.28	for targeted, monitored communications including potential communications between the employee and competitors and other insider risk behaviors, especially copying IP, downloading IP, or other efforts to acquire IP prior to insider departure from the organization
IT1.1	attempted unauthorized account creation
IT1.2	attempted unauthorized sharing of shared accounts and use of authorized shared accounts
IT1.3	logs, including user account, resources accessed, and physical and/or logical location of access attempts (MAC and IP addresses); point of logical system entry (router, VPN, or firewall ID); workstation ID; date; and time
IT1.8	attempts to connect unauthorized systems/devices to the organization's systems
IT2.2	abnormal activities related to log file access—Log aggregation can uncover trends and anomalies, and automated alerts can notify personnel of abnormal activities in excess of established thresholds.
IT2.3	specified logging and monitoring activities on remote connection—Log analysis and audit should then be done within the SIEM system.
IT2.4	successful and unsuccessful login attempts to IT systems—These should be logged and sent to the SIEM system, which should review them for anomalous login activity. The logs should include access date and time, success/failure, system from which the attempt was initiated, and user account.
IT2.5	specified, monitored processes deviating from normal activities—Data should be audited at the SIEM system.
IT2.7	alterations of critical data
IT3.1	unauthorized modification/deletion of critical data

Capability sequence	Data that goes to SIEM system for logging, analysis, and alerts
IT3.3	unauthorized modification of operational systems, deployed production software, and production systems (e.g., registry changes), even if performed by system administrators
IT3.4	unauthorized addition of new hardware to computer and network systems
IT3.5	logs of critical systems to track access and activity of system administrators
IT4.3	technological access logs to track employees and/or trusted business partners who attempt to access backup copies
IT5.3	deviations from baselined systems activities
IT5.4	abnormal (deviations from the baseline) behavior as it relates to after-hours access
IT5.7	monthly reviews of access logs to uncover unauthorized access attempts and adjust alerting parameters for such attempts (the reviews may be done by a SIEM system, as well as the alerts)
IT5.8	local access attempts to workstations—Review workstation login logs for deviations from normal login attempts.
IT5.9	abnormal download traffic patterns—logs of increased monitoring of the activity of accounts belonging to terminating and suspended employees, use of mass copying software (backup utilities, CD burners, etc.) by unauthorized employees, detected unauthorized downloads and installations of applications, and detected known malicious software on systems
IT5.10	encrypted traffic logs sent to a central log correlation engine (can be a SIEM)
IT6.3	account activity of monitored terminating employees
IT6.8	logs and other evidence that may enable the organization to take legal action against terminated employees attempting to exploit unauthorized, open connections to the organization's network
IT7.1	established baselines of normal system-activity levels, detected deviations from normal system-activity levels
IT7.4	detected network connections that use unauthorized communication methods
IT7.5	baseline of normal network activity, DoS or distributed denial-of-service (DDoS) attacks via firewall/IDS, and deviations above normal network activity levels
PS1.1	unauthorized physical access by employees to critical or sensitive areas and access control system logs of all access attempts (logs can be reviewed by the SIEM)
SE1.3	unauthorized access to high-value software assets
TBP1.7	logs and monitoring information from contractors
TBP1.8	monitoring of all contractors whose potential misuse of sensitive and confidential information could harm the organization

4 Conclusions and Future Efforts

4.1 Future Research

CSPs are in the process of further understanding how deployed administrative and technical controls within their existing environment can be refined to assist with insider threat detection. CERT research indicates that current practices relative to insider threat management programs are immature. However, CSPs are seeking meaningful guidance from control frameworks such as those proposed by the ISO/IEC, NIST, FedRAMP, CSA, CERT Division, and others to improve and grow current insider threat capabilities.

As described throughout this report, the CERT Division's analysis indicates that CSPs could benefit from a number of future research initiatives, including but not limited to the following:

- Examine the administrative and technical process challenges to account for mobile device and/or MDM data integration into CSP SIEM platforms for correlation and analysis. The use of mobile devices will only continue to grow, and understanding how to capture and utilize the DI they generate (or should generate in the future) to assist with insider threat detection, data exfiltration, and other security issues will be beneficial.
- Develop signatures, based on ITA workbook capabilities, that can be implemented within IDS/IPS and/or SIEM systems to help CSPs detect possible insider attacks.
- Enhance the current understanding of the techniques informed insiders may use to evade discovery. CSPs could use a taxonomy of insider threat actors and their motivations to guide their development of a profile of attributes, relevant HR measures, and technical indicators to identify and mitigate insider threat behaviors. The sheer scale of cloud computing packet and log data could give rise to new capabilities for real-time detection of insider threats.

CSPs are eager to adopt insider threat management processes, but specific guidelines and standards outlining best practices within the cloud sector are needed both to accelerate adoption on a greater scale and to respond to increasing scrutiny regarding insider breaches.

4.2 Expanding the Relationship With and Among Cloud Service Providers

In both phases of the research, we hoped the CERT Division might function as a trusted intermediary between CSPs, which ordinarily might be reluctant to share cybersecurity information and techniques with their competitors. The CERT Division's parent institution, the SEI, is a nonprofit, federally funded research and development center (FFRDC) chartered by the U.S. Department of Defense (DoD). The CERT Division has historically served as a trusted repository of cybersecurity vulnerability information, such as information about viruses and attacks, and it has helped organizations share cybersecurity information for the benefit of their entire industry [Longstaff 1997, CERT 2012]. The CERT Division's charter forbids it from competing with industry. Both phases of this CSP research project have been sponsored by DHS, all potential participants were assured that their responses would be aggregated and anonymized, and the researchers on our team all hold U.S. DoD security clearances. Some CERT researchers

have found that participants are more open to an organization like the CERT Division, as opposed to a governmental organization with regulatory power.

Going forward, the CERT Division hopes to expand its relationships with CSPs, as this could lead to greater participation in future research efforts and expand the CERT Division's ability to anonymize and share a greater breadth of practice-related information. These efforts might also enable and encourage CSPs to engage with each other for the benefit of the entire industry.

Potential CSP partners in CERT research might be reassured by greater visibility of DHS's involvement in the project, achieved perhaps by DHS personnel instigating the initial requests for participation, CERT researchers inviting DHS personnel to participate in the group interviews, or CERT researchers asking DHS to help organize a symposium at one of its secure facilities.

The CERT Division could also help establish an industry consortium where CSPs can efficiently share cybersecurity threats and mitigations for the benefit of all participants. CSPs may have programs to address the insider threat vector, yet still lack tools and processes to support their efforts. Additionally, CSPs do not regularly share, if at all, industry-based insider threat best practices and lessons learned. A CSP Information Sharing and Analysis Center (CSP-ISAC) could serve as a trusted entity, established by both government and commercial CSPs, to provide comprehensive sector analysis. Results could then be shared within the sector and with other ISACs to provide risk mitigation, incident response, and relevant alerting data points. ISACs have long been established in other sectors, such as financial services, higher education, and electric utilities. The overarching goal of the ISAC is to provide users with accurate, actionable, and relevant information.

The CERT Division could also develop an annual symposium with high-level leaders from the CERT Division, academia, government organizations, and CSPs' cybersecurity experts. The focus of this CERT CSP symposium would be on CSP cybersecurity threats and mitigations, and it would include sessions that would enable secure information sharing. All attendees could benefit from networking with each other as well as mutually and securely exchanging CSP cybersecurity information. CSP industry leaders could offer feedback and possibly solicit new research for challenges they face. We can imagine the CSP symposium spawning deep, collaborative relationships that might involve the exchange of visiting researchers.

Bibliography

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

[Abboud 2013]
Abboud, Leila & Sandle, Paul. "Analysis: European Cloud Computing Firms See Silver Lining in PRISM Scandal." *Reuters*, June 17, 2013. http://www.reuters.com/article/2013/06/17/us-cloud-europe-spying-analysis-idUSBRE95G0FK20130617

[Babcock 2013]
Babcock, Charles. "NSA's Prism Could Cost U.S. Cloud Companies $45 Billion." *Information Week*, August 15, 2013. http://www.informationweek.com/cloud-computing/infrastructure/nsas-prism-could-cost-us-cloud-companies/240159980

[Bejtlich 2013]
Bejtlich, Richard. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response.* No Starch Press, 2013.

[CERT 2012]
The CERT Division. *The CERT® Program FAQ.* http://www.cert.org/faq/ (2012).

[CERT Insider Threat Center 2011]
CERT Insider Threat Center. *Insider Threat Control: Using a SIEM Signature to Detect Potential Precursors to IT Sabotage*. Software Engineering Institute, Carnegie Mellon University, 2011. http://www.cert.org/archive/pdf/SIEM-Control.pdf

[Department of Commerce 2012]
Department of Commerce. *Welcome to the U.S.-EU Safe Harbor.* http://export.gov/safeharbor/eu/eg_main_018365.asp (2012).

[Department of Defense 2013]
Department of Defense, Defense Science Board. *Task Force Report: Cyber Security and Reliability in a Digital Cloud.* Department of Defense, 2013. http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf

[Department of Justice 2013]
Department of Justice, Office of Public Affairs, Criminal Division. *US Army Sergeant Pleads Guilty in Georgia to Stealing Identity Information from US Army Computer System*. http://www.justice.gov/opa/pr/2013/July/13-crm-812.html (2013).

[Flynn 2013]
Flynn, Lori; Huth, Carly; Trzeciak, Randall; & Buttles-Valdez, Palma. *Best Practices Against Insider Threats in All Nations* (CMU/SEI-2013-TN-023). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59082

[Gallagher 2013]
Gallagher, Sean. "PRISM Revelations Result in Lost Business for US Cloud Companies." *Ars Technica*, July 26, 2013. http://arstechnica.com/tech-policy/2013/07/prism-revelations-result-in-lost-business-for-us-cloud-companies/

[Gorman 2013]
Gorman, Siobhan. "NSA Officers Spy on Love Interests." *The Wall Street Journal*, August 23, 2013. http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/

[ISO/IEC 2005]
International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). *ISO/IEC 27001:2005, Information Technology—Security Techniques—Information Security Management Systems—Requirements*. http://bsi.learncentral.com/shop/Course.aspx?id=12772&name=BS+ISO%2fIEC+27001%3a2005 (2005).

[Kastrenakes 2013]
Kastrenakes, Jacob. "Snowden Reportedly Had Access to Classified NSA Documents Even as a Dell Contractor." *The Verge*, August 16, 2013. http://www.theverge.com/2013/8/16/4628334/snowden-document-collection-began-dell-2012

[Longstaff 1997]
Longstaff, Thomas A.; Ellis, James T.; Hernan, Shawn V.; Lipson, Howard F.; McMillan, Robert D.; Pesante, Linda Hutz; & Simmel, Derek. *Security of the Internet.* https://www.cert.org/encyc_article/tocencyc.html (1997).

[Moore 2009]
Moore, A. P.; Cappelli, D. M.; Caron, T.; Shaw, E.; & Trzeciak, R. F. "Insider Theft of Intellectual Property for Business Advantage: A Preliminary Model." *Proceedings of the 1st International Workshop on Managing Insider Security Threats (MIST2009).* Purdue University, West Lafayette, IN, June 2009. http://www.cert.org/insider_threat/docs/Insider_Theft_of_IP_Model_MIST09.pdf

[Moore 2012]
Moore, A. P.; Hanley, M.; & Mundie, D. "A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders." *Proceedings of the 18th Conference on Pattern Languages of Programs (PLoP'11)*. Portland, OR, Oct. 2011. ACM, 2012. http://www.hillside.net/plop/2011/papers/D-6-Moore.pdf

[Mundie 2012]
Mundie, D. & Moore, A. P. "A Pattern for Trust Trap Mitigation." Proceedings of the 18th Conference on Pattern Languages of Programs (PLoP). *Proceedings of the 18th Conference on Pattern Languages of Programs (PLoP'11)*. Portland, OR, Oct. 2011. ACM, 2012. http://www.hillside.net/plop/2011/papers/D-23-Mundie.doc

[Naughton 2013]
Naughton, John. "Edward Snowden's Not the Story. The Fate of the Internet Is." *The Observer*, July 27, 2013. http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet?

[NIST 2011]
National Institute of Standards and Technology (NIST). *NIST Special Publication 500-299: Cloud Computing Security Reference Architecture*. NIST, 2011.

[Obama 2012]
Obama, Barack. *Presidential Memorandum -- National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.* The White House, Office of the Press Secretary, November 21, 2012. http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

[Porter 2013]
Porter, Greg. *Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase I* (CMU/SEI-2013-TN-020). Software Engineering Institute, Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=69709

[Ristenpart 2009]
Ristenpart, Thomas; Tromer, Eran; Shacham, Hovav; & Savage, Stefan. *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds.* ACM, 2009. http://www.cs.cornell.edu/courses/cs6460/2011sp/papers/cloudsec-ccs09.pdf

[Rocha 2011]
Rocha, Francisco & Correia, Miguel. "Lucy in the Sky Without Diamonds: Stealing Confidential Data in the Cloud." *Proceedings of the 1st International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV, with DSN'11)*, Hong Kong, June 2011. IEEE, 2011.

[Ross 2008]
Ross, Brian; Walter, Vic; & Schecter, Anna. "Exclusive: Inside Account of U.S. Eavesdropping on Americans." *ABC News*, October 9, 2008. http://abcnews.go.com/Blotter/story?id=5987804&page=1#.UbNXP0Cq-2U

[Samson 2013]
Samson, Ted. "Germany Joins in Voicing Distrust of U.S.-Based Cloud Services." *InfoWorld*, July 3, 2013. http://www.infoworld.com/t/data-security/germany-joins-in-voicing-distrust-of-us-based-cloud-services-222094

[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://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=34017

[Thibodeau 2013]
Thibodeau, Patrick. “Snowden Revelations May Cost U.S. Cloud Providers Billions, Says Study.” *Computerworld*, August 9, 2013. http://www.computerworld.com/s/article/9241489/Snowden_revelations_may_cost_U.S._cloud_providers_billions_says_study

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	January 2014	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase II, Expanded Analysis and Recommendations	FA8721-05-C-0003

6. AUTHOR(S)

Lori Flynn, Greg Porter, Chas DiFatta

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-030

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	

11. SUPPLEMENTARY NOTES

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

13. ABSTRACT (MAXIMUM 200 WORDS)

Throughout the third quarter of 2013, researchers in the CERT® Insider Threat Center, part of the Carnegie Mellon Software Engineering Institute, contacted commercial and government cloud service providers (CSPs) to better understand the administrative and technical risks posed by CSP insiders and the countermeasures that CSPs are considering and deploying to identify and mitigate insider attacks. Based on the insight obtained from participating CSPs, CERT researchers have examined how existing CSP insider threat management practices may be improved. Researchers also examined the CERT Division's Insider Threat Assessment workbooks to identify some data types useful for CSP security information and event management (SIEM) systems, specifically for mitigating insider threats. A table listing those identified data sources may be of use for CSPs adding logging, analysis, and alerts to their SIEM systems. This report contains observations obtained from interview and survey responses of participating CSP personnel, considerations for improving insider threat mitigation processes, and current challenges within the CSP community as observed by the Insider Threat Center team.

14. SUBJECT TERMS	15. NUMBER OF PAGES
cloud, cloud service provider, CSP, controls, processes, interview, survey, ITA workbooks	45

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