@ISACA
RELEVANT, TIMELY NEWS
Volume 7, 26 March 2014

Five Ways to Limit Insider Threats

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

Insider threat has become a key concern for many organizations, especially in the wake of the recent US National Security Agency (NSA) disclosures by Edward Snowden. Traditionally, the primary threat and focus for security activities has been the motivated and capable external adversary. The idea of an insider or third-party vendor in any way being untrustworthy or carrying out malicious activities against his/her organization was an unaddressed possibility.

Read More

Normalization of Deviance: North America CACS Keynote Preview

Former Space Shuttle Astronaut Mike Mullane will deliver the closing keynote address at ISACA's North America CACS in April. Mullane's session will focus on a concept he calls the normalization of deviance.

Read More

New Knowledge Center Community Topic: COBIT 5 Assessment

COBIT 5 Assessment joins 2 other COBIT® 5 topics in the Knowledge Center: COBIT 5—Use It Effectively and COBIT 5 Implementation. Like COBIT 5—Use It Effectively, the COBIT 5 Assessment Knowledge Center topic will be open to ISACA® members and nonmembers who are registered web site users in an effort to provide a community for those who are assessors or are interested in becoming COBIT 5 Certified Assessors.

Read More

Open Badge Rollout to Be Complete by April

In February, ISACA announced the introduction of open badges for certification holders. An open badge is a web-enabled icon that allows you to display your ISACA certification on social and professional networking sites, in emails, or on personal web sites, with single-click verification (linking to metadata that describe your credential and the rigorous process required to earn it).

Read More

New COBIT-related Audit Programs Available

It is becoming increasingly important for assurance professionals to be able to deliver solutions and services in a cost-effective manner, comply with legal and regulatory requirements, and communicate with stakeholders effectively. To meet these needs, ISACA is creating audit/assurance programs for COBIT 5 processes, based on the generic structure developed in *COBIT® 5 for Assurance*.

Read More

Book Review: *The Computer Incident Response Planning Handbook*

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

The Computer Incident Response Planning Handbook, by N.K. McCarthy, aims to provide the

reader with the skills to create effective and appropriate computer incident response plans. Computer incident response was once the sole responsibility of the IT department, but as it has become clear that the consequences of a computer incident can threaten an enterprise's very existence, directors are now being held more accountable.

Read More

Five Ways to Limit Insider Threats

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

Insider threat has become a key concern for many organizations, especially in the wake of the recent US National Security Agency (NSA) disclosures by Edward Snowden. Traditionally, the primary threat and focus for security activities has been the motivated and capable external adversary. The idea of an insider or third-party vendor in any way being untrustworthy or carrying out malicious activities against his/her organization was an unaddressed possibility. Unfortunately, in many cases, an insider with motivation and limited capability has a greater opportunity to cause material damage to an organization than the motivated and highly capable external adversary. These individuals have the means, methods and opportunity to successfully attack an organization.

The idea of not trusting employees and vendors to act in the best interests of the organization is often culturally unacceptable. Unfortunately, even the most trusted and respected insider can have a bad day or become a bad actor. Here are 5 ways that an organization can limit the effects of insider threats:

1. **Trust, but verify**—Former US President Ronald Reagan said it best in his approach to peace during the Cold War: "Trust, but verify." The activities of an organization's individuals and systems that have access to sensitive information infrastructure or data assets should be monitored to ensure internal actors are working in the best interest of the organization. This monitoring does not have to be presented or operated as a negative, "big brother" oversight. On the contrary, if implemented and presented properly, these measures can actually be seen as a positive practice for individuals with this type of access.
2. **Privileged user management**—The most dangerous insiders are those who have privileged access to sensitive information infrastructure and data assets as part of their job responsibilities. By following a policy of least-privileged access, wherein individuals are given only the minimum level of access required to perform their role, organizations can minimize the population of potentially threatening users with the ability to have a material impact on their business. The privileged activities of this population of users should then be diligently monitored to ensure that they are always working in the best interests of the organization. One of the most effective methods to accomplish this is to establish segmented networks, environments and systems that will be used for privileged activities.

3. **Segmentation of duties**—No one person or system should have the ability to materially impact an organization. In many cases, insider threats are amplified due to a high level of access, responsibilities and/or capabilities that individuals or systems are provided. By segmenting key duties and responsibilities, collusion between individuals will have to exist to successfully carry out a malicious activity that can materially impact the organization. It is recommended to include a business risk-based review of roles, credentials and their associated entitlements for both users and systems as part of an organization's risk-assessment activities. This review should include a revision of current segmentation capabilities and the identification of opportunities for new and enhanced segmentation of responsibilities and capabilities for users and systems.
4. **Third-party monitoring**—Insiders may not always be those who are employees or systems that are employed or owned by the organization. Third parties and their employees are often provided extensive and trusted access to information infrastructure and data assets of the organization to effectively provide their services. Third parties may be targeted by adversaries who assume these organizations may not maintain the same level of defensive capabilities as the target organization and recognize that third-party staff lack any emotional connection to the target organization. Vendor compliance reviews can be helpful in ensuring that appropriate controls are in place to oversee privileged user access and monitoring by service providers and third parties, but it is often difficult for organizations to ensure that consistent and effective capabilities exist in this area. For this reason, service providers and third parties that have this type of access should be categorized at the highest risk levels, and their actions and activities should be monitored with the same, if not a stricter, level of oversight and control than the organization utilizes for internal staff and systems.
5. **Behavior monitoring**—It is often the case that insiders who carry out malicious activities demonstrate a change in behavior, personality or activities just before or while they are carrying out their malicious activities. Many insider threats can be diffused by providing training to management on behaviors that may be indicative of an impending or ongoing malicious activity by a trusted insider. Common behaviors to monitor include abrupt changes in personality or work behaviors, access to materials or systems that are not typical for a user's work activities, or emotional disengagement from the organization and peers. Users, peers and system owners are often the greatest source of intelligence about insider threats. But these individuals may feel unable or afraid to report this information due to a fear of reproach or being viewed as a snitch. Thus, it is important to establish a confidential and/or anonymous means for individuals to communicate their concerns to independent authorities or business leaders that will allow them to feel safe and comfortable.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

Normalization of Deviance: North America CACS Keynote Preview

Former Space Shuttle Astronaut Mike Mullane will deliver the closing keynote address at ISACA's **North America Computer Audit, Control and Security (CACS) Conference** in April. Mullane's session will focus on a concept he calls the normalization of deviance.

"Normalization of deviance is a phenomenon in which individuals or teams repeatedly accept a deviance from best practices until that deviance becomes the norm," he says. "Usually, the acceptance of the deviance occurs because the individual/team is under pressure (e.g., budget, schedules) and perceives that it will be too difficult to adhere to the best-practice standard while executing the mission."

By taking shortcuts that usually work, teams begin to make these shortcuts the norm, which could have disastrous consequences. In the space program, for example, normalization of deviance can have costly impacts, such as the Space Shuttle Challenger tragedy.

In addition to having insights on the normalization of deviance, Mullane has seen how technology has evolved over the course of the 30-year span of the shuttle program and will also discuss the program's reliance on IT and how it has changed over the years.

Read the full Q&A with Mullane in the **ISACA Now Blog**, or visit the **North America CACS** page of the ISACA® web site to learn more about and register for the conference.

New Knowledge Center Community Topic: COBIT 5 Assessment

COBIT 5 Assessment joins 2 other COBIT® 5 topics in the Knowledge Center: COBIT 5—Use It Effectively and COBIT 5 Implementation. Like COBIT 5—Use It Effectively, the COBIT 5 Assessment Knowledge Center topic will be open to ISACA® members and nonmembers who are registered web site users in an effort to provide a community for those who are assessors or are interested in becoming COBIT 5 Certified Assessors.

The creation of the COBIT 5 Assessment topic was suggested by topic leader Ayilur Ramnath who recently passed his assessor exam and is eager to discuss how to assess and report. Learn more and discuss the benefits (to individuals and enterprises) of becoming a certified

assessor in the new COBIT 5 Assessment topic. Join the **COBIT 5 Assessment community** today.

Open Badge Rollout to Be Complete by April

In February, ISACA® announced the **introduction of open badges** for certification holders. An open badge is a web-enabled icon that allows you to display your ISACA certification on social and professional networking sites, in emails, or on personal web sites, with single-click verification (linking to metadata that describe your credential and the rigorous process required to earn it).

The badges are based on a new open standard for communicating learning called **Mozilla Open Badges**. All certification holders will receive an email about open badge enrollment by 31 March 2014. Learn more on the **Open Badges** page of the ISACA web site. Questions? Contact **badges@isaca.org**.

New COBIT-related Audit Programs Available

It is becoming increasingly important for assurance professionals to be able to deliver solutions and services in a cost-effective manner, comply with legal and regulatory requirements, and communicate with stakeholders effectively.

To meet these needs, ISACA® is creating audit/assurance programs for COBIT® 5 processes, based on the generic structure developed in *COBIT® 5 for Assurance*. The **5 programs for the governance domain** Evaluate, Direct and Monitor (EDM) are the first to be issued. This first set will allow practitioners to ensure governance framework setting, benefits delivery, risk optimization, resource optimization and stakeholder transparency.

These programs are fully aligned with COBIT 5 and reference all 7 enablers. Over the next several months, ISACA will release 34 audit/assurance programs, which were developed by assurance professionals and have undergone peer review. Programs for other COBIT domains are planned for release: Align, Plan and Organize (April 2014); Build, Acquire and Implement (June 2014); and Deliver, Service and Support (June 2014).

These in-depth programs were designed to be flexible. The detailed structure of these programs enables assurance professionals to make their own scoping decisions. These programs are complimentary and customizable Microsoft Word downloads for ISACA members and available for purchase by nonmembers in the **ISACA Bookstore**. To download or purchase these programs, visit the **Research Deliverables** page of the ISACA web site.

Information on recently released and upcoming research projects is posted on the **Current Projects** page of the ISACA web site.

Book Review: *The Computer Incident Response Planning Handbook*

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

The Computer Incident Response Planning Handbook, by N.K. McCarthy, aims to provide the reader with the skills to create effective and appropriate computer incident response plans.

Computer incident response was once the sole responsibility of the IT department, but as it has become clear that the consequences of a computer incident can threaten an enterprise's very existence, directors are now being held more accountable. Directors have to be aware that a serious computer incident could result in a number of negative consequences for their enterprise, such as reputational damage or regulatory fines.

The obligations of directors filter down to those responsible for developing and maintaining standards and procedures. *The Computer Incident Response Planning Handbook* is useful for anyone who is responsible for computer incident response—directly or indirectly. The publication is written for nontechnical people and does not require the reader to be a technical expert.

The Computer Incident Response Planning Handbook is a combination reference guide and how-to publication. It is organized into four parts: The Threat Landscape, Planning for Crisis, Plan Development: Data Breach, and Plan Development: Malware. The first 2 parts provide the reader with context and explain the theory and concepts behind computer incident response, while the latter 2 parts take the reader through the planning and development of useable malware and data breach plans. The final chapter of the book allows the author to explain and explore a number of information security paradigms. This is a short, but useful and thought-provoking chapter that helps the reader consider and explore the future scenarios for computer incident response.

The publication supports compliance with standards such as the Payment Card Industry Data Security Standard (PCI DSS), the US Health Insurance Portability and Accountability Act (HIPAA), and the US Sarbanes-Oxley Act; explains the role of COBIT® in IT governance and control; and links COBIT to other standards such as ITIL and the ISO 27000 series.

This book is comprehensive and logically organized. By the end of the book, readers should feel confident in designing and implementing their own computer incident action plans. The book also includes a list of useful online resources, although not comprehensive, that supports

the publication and provides additional help and advice.

The publication's main strength is that it provides sound and practical guidance on computer incident response plans that can help to bolster an enterprise's security.

Computer Incident Response Planning Handbook is available from the ISACA® Bookstore. For information, see the ISACA Bookstore Supplement in the latest issue of the ***ISACA Journal***, visit the **ISACA Bookstore** online or email **bookstore@isaca.org**.

Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI, is the group information security officer (ISO) at AEGON UK. Richardson has more than 25 years of experience in IT, information security, audit and risk.

©2014 ISACA. All rights reserved.