@ISACA
RELEVANT, TIMELY NEWS
Volume 10, 7 May 2014

Who Owns Loss Owns Risk

By Jack Freund, Ph.D., CISA, CISM, CRISC

Identifying risk ownership may appear straightforward, but it is important to that ensure it has been assigned to the correct individual. Too often, any risk having to do with IT is assigned to someone in the IT function.

Read More

Cybersecurity Nexus: Everything You Need on Cybersecurity

To meet the growing demand for cybersecurity professionals, ISACA® has launched Cybersecurity Nexus (CSX), which is a central location where professionals can find comprehensive cybersecurity guidance.

Read More

CISA and ISACA Standards Used in New Audit Guidance

New audit guidance has been issued by the German Federal Office for Information Security (BSI) and the ISACA Germany Chapter. This guidance lists requirements for persons who perform an assessment and it refers to IS Audit and Assurance Standard 1006 (Proficiency),

which, in turn, acknowledges the Certified Information Systems Auditor® (CISA®) certification.

Read More

ISACA Supports Knowledge Sharing Through CSR Program

As its second contribution under the new corporate social responsibility (CSR) program, ISACA donated US $20,000 to the United Nations Educational, Scientific and Cultural Organization's (UNESCO) Building Knowledge Societies Program.

Read More

Maximize the Value of the Cloud With COBIT 5

Controls and Assurance in the Cloud: Using COBIT® 5 provides practical guidance for enterprises using or considering using cloud computing. This book identifies cloud-related risk and controls and provides a governance and control framework based on COBIT 5 and an audit program using *COBIT® 5 for Assurance*.

Read More

Book Review: *Hacking Exposed Mobile Security Secrets and Solutions*

Reviewed by Upesh Parekh, CISA

As with most technological advancements, there are growing concerns about the security of mobile computing. *Hacking Exposed Mobile Security Secrets and Solutions* focuses on some of the known and unknown vulnerabilities around mobile computing and provides suggested remedies to these issues.

Read More

Who Owns Loss Owns Risk

By Jack Freund, Ph.D., CISA, CISM, CRISC

Identifying risk ownership may appear straightforward, but it is important to that ensure it has been assigned to the correct individual. Too often, any risk having to do with IT is assigned to someone in the IT function. To determine if this risk placement is correct, take the following example scenario to help identify the real risk owner.

First, assume that we are evaluating the risk associated with the compromise of public-facing e-commerce systems. If these systems are hacked, cybercriminals will have access to payment cards and sensitive customer information. A perfunctory evaluation might identify that, since the e-commerce systems are managed by IT (and, technically, are IT), someone from IT should own the risk. In fact, that same person would be responsible for implementing controls that would prevent the attack from succeeding.

Further assume that an attack does happen and the server is compromised along with customers' payment and personal information. As a result, management decides to fire the person in charge of the e-commerce system. But, the fallout from the hack continues to grow as customers avoid the company's products and services. So, management decides to fire the chief information officer (CIO). In fact, things get so bad that management decides that the entire IT department is to blame, so they are all fired.

In this fictitious and unrealistic scenario, one thing remains true: The impact of the loss is not felt by anyone in IT. Oh, they have lost their jobs and that hurts, but the impact to the business remains. Those lost customers still are not coming back, and the lack of sales as a result is very real to the business. It is for this reason that the following adage is useful for identifying the real risk owner: Who owns loss owns risk.

In the example here, the owner of the risk should rightfully be someone on the business side of the organization. In most cases, it should be someone responsible for products and services who will own the loss if things go wrong. Others may be responsible for helping to keep that from happening, but ownership ought to be retained by the business side of your organization, not IT.

Jack Freund, Ph.D., CISA, CISM, CRISC, is an IT risk manager for TIAA-CREF and chairs ISACA's CRISC Test Enhancement Subcommittee.

Cybersecurity Nexus: Everything You Need on Cybersecurity

To meet the growing demand for cybersecurity professionals, ISACA® has launched Cybersecurity Nexus (CSX), which is a central location where security professionals can find comprehensive cybersecurity guidance. CSX offers training, education, research, certification and career development.

Under this program, ISACA is offering the new Cybersecurity Fundamentals Certificate. This certificate, ideal for anyone interested in entering the cybersecurity field, aligns with the US National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) and the Skills Framework for the Information Age (SFIA). Optional workshops and the first exams for this certificate will be held at the 2014 **European Computer Audit, Control and Security and Information Security and Risk Management Conference** (EuroCACS/ISRM) in September and **North America Information Security and Risk Management (ISRM) Conference** in November.

Additional elements of the CSX program include a cybersecurity practitioner certification for which the first exam is scheduled for mid-2015.

For more information on the program, visit the **Cybersecurity Nexus** page of the ISACA web site.

CISA and ISACA Standards Used in New Audit Guidance

New audit guidance has been issued by the German Federal Office for Information Security and the ISACA® Germany Chapter to help organizations assess their security exposure and security controls with regard to cyberattacks. This guidance uses the Certified Information Systems Auditor® (CISA®) certification by referring to IS Audit and Assurance Standard 1006 (Proficiency), which acknowledges the CISA certification.

This guidance also includes various references to other ISACA publications, including additional IS Audit and Assurance Standards, *Transforming Cybersecurity Using COBIT® 5* and *Responding to Targeted Cyberattacks*, as well as a mapping of basic security controls to the COBIT 5 process reference model. At the moment, only a **German version** is available, but an English translation is planned.

ISACA Supports Knowledge Sharing Through CSR Program

As its second contribution under the new corporate social responsibility (CSR) program, ISACA® donated US $20,000 to the United Nations Educational, Scientific and Cultural Organization's (UNESCO) Building Knowledge Societies Program.

"UNESCO is grateful to ISACA for its support," said Indrajit Banerjee, director of the Knowledge Societies Division of UNESCO. "ISACA's contribution to UNESCO will be utilized to further its Building Knowledge Societies Program, and particularly for its activities on Open Solutions, which enable information and knowledge to be openly shared providing strategic cross-cutting opportunities to improve the quality of decision making and to facilitate policy dialogue knowledge sharing as well as capacity building."

This donation comes from the CSR program's support of a cause—international portion, and is the final donation in this category for 2014 under the CSR. In addition to donations to international organizations, the CSR program, which is operating on a 3-year pilot basis, also allows ISACA volunteers, members and staff to apply for ISACA funding to be donated to local/regional organizations and activities. The criteria for qualifying to receive funding and a link to the application form are available on the **Criteria for Support of a Cause** page of the ISACA web site.

To learn more about this program, visit the **Corporate Social Responsibility Program** page of the ISACA web site.

Maximize the Value of the Cloud with COBIT 5

Controls and Assurance in the Cloud: Using COBIT® 5 provides practical guidance for enterprises using or considering using cloud computing. This book identifies cloud-related risk and controls and provides a governance and control framework based on COBIT 5 and an audit program using *COBIT® 5 for Assurance*.

Although cloud computing can provide great value to businesses, it is important to consider the risk associated with it. This book explains the risk created by using cloud services, how to mitigate this risk and how to maximize value in the cloud. This information can assist enterprises in assessing whether the risk that comes with cloud computing is within an acceptable level.

For enterprises that already use cloud computing, this publication contains information on how to create controls and governance mechanisms for the cloud. This book suggests many monitoring mechanisms, and readers can create a customized monitoring system by selecting which monitoring techniques to implement.

A **PDF of the book** and a **Microsoft Word** file of the audit program are available as complimentary downloads for members. Print and PDF versions of the book and the audit program used in the book are available in the **ISACA® Bookstore**.

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

Book Review: *Hacking Exposed Mobile Security Secrets and Solutions*

Reviewed by Upesh Parekh, CISA

There are about **6.8 billion mobile subscriptions** in the world today. In turn, more people have mobile devices than desktops and laptops. Not surprisingly, there are more and more mobile applications being developed worldwide. In May 2012, more than **10 percent of web site hits** came from handheld mobile devices.

As with most technological advancements, there are growing concerns about the security of mobile computing. *Hacking Exposed Mobile Security Secrets and Solutions,* by Neil Bergman, Mike Stanfield, Jason Rouse, Joel Scambray, Sarath Geethakumar, Swapnil Deshmukh and Scott Mats, focuses on some of the known and unknown vulnerabilities around mobile computing and provides suggested remedies to these issues. This book is targeted to technical people, especially those who are responsible for building, testing, assessing and assuring the security of mobile computing.

To understand the threats to mobile computing, it is important to understand the mobile risk ecosystem, which is similar to, but not exactly the same as, conventional computing. The first chapter of the book covers this ecosystem and the next chapter deals with cellular networks and related vulnerabilities.

The following 2 chapters cover 2 major operating systems: iOS and Android, as these cover a large market share. The book then gives numerous examples and remedies of known mobile malware and covers mobile services and mobile web, mobile device management, and mobile application development security. The book concludes with coverage of the weaknesses related to mobile payments.

By and large, the fundamental concepts around mobile computing are similar to conventional

computing. However, the dissimilarities cause most of the issues. The authors discuss these dissimilarities thoroughly. The book cites many real-life examples and includes references to numerous related web sites. This book points to the vulnerabilities of mobile devices and provides countermeasures to these weaknesses.

Hacking Exposed Mobile Security Secrets and Solutions 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**.

Upesh Parekh, CISA, is a governance and risk professional with more than 10 years of experience in the fields of IT risk management and audit. He is based in Pune, India, and works for Barclays Technology Centre, India.