ISACA
Serving IT Governance Professionals
Greater Kansas City Chapter

August 2009 Volume 2, Issue 1

Celebrating 25 Years!!

2009 - 2010 Officers:

President
Kevan Brewer

Vice-President
Jerry Wistrand

Associate VP
Alfie Mahmoud

Secretary
Wendy Dobratz

Treasurer
Nila Holmquist

Director
Jim Wilcox

Director
Jennifer Harper

Director
Mike Connors

In this issue:

September Meeting Details

.Securing Administrative Passwords

Interested in how to securely manage shared privileged accounts, such as Windows Local Administrator, Oracle Sys/System, SQL-Server SA and Cisco Enable? These identities are the most powerful and sensitive identities in the organization. Mismanagement of these accounts, which leads to their exploit, loss or exposure, might result in a failed audit, security catastrophe and long recovery process.

This presentation will cover:

- Challenges with the management of shared administrative passwords
- Risks involved with common practices employed by businesses
- Achieving compliance with regulatory requirements ensuring audit and accountability
- Reducing the risk associated with insider threats
- Minimizing the loss of sensitive information
- Decreasing administrative overhead

Date: September 10, 2009

Time: 11:30 AM - 12:00 PM Registration **|** 12:00 - 1:00 PM Lunch **|** 1:00-3:00 PM Program

Location: Figlio's Tower | 209 West 46th Terrace | Kansas City | MO | 64112

Price: $35 members | $10 Students | $50 guests

CPE: 2 Credits

Menu: TBD

Speaker Bio:

Dave Adamczyk, Channel Sales Manager, Cyber-Ark Software

Dave has spent the past four years with Cyber-Ark Software working as a Channel Sales Manager. He has ten years of experience working with large enterprises in the areas of security, software, and networking. Formerly, he was a Software Support Engineer and Service Account Manager with Sun Microsystems working directly with their enterprise customers. Dave holds a B.S. in Computer Science from Providence College in Rhode Island as well as a Masters Degree in Business Administration from Northeastern University in Boston.

Registration is currently open on our website at http://www.isaca-kc.org/

Feedback Forum

If you have suggestions regarding presentation topics, speakers or locations, please contact Carman Kesner, our Programs Chair.

2009 - 2010 Monthly Meeting - SAVE THE DATE

Sept. 10, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Securing Administrative Passwords" - Dave Adamczyk, Cyber-Ark
October 8, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
November 12, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Hoodlums to Hackers – Jeff Lanza, former FBI Special Agent
December 10, 2009	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
January 14, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
February 11, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
March 11, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
April 8, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation TBD
May 13, 2010	11:30 – Noon Registration Noon – 1:00 PM Lunch 1:00 – 3:00 PM Presentation	Presentation Annual Business Meeting

CISA and CISM Exams Information

The Certified Information Systems Auditor (CISA) is ISACA's cornerstone certification. The CISA certification has been earned by more than 60,000 professionals since inception and is for the IS audit, control, assurance and/or security professionals who wish to set themselves apart from their peers. Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

The Certified Information Security Manager (CISM) certification is a unique management focused certification that has been earned by over 9,000 professionals since its introduction in 2003. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise's information security program. CISM defines the core competencies and international performance standards that those who have information security management responsibilities must master.

The IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. More than 200 CGEIT certificates have been awarded. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by a "job practice" consisting of IT governance related tasks and knowledge. Earning this designation will enable professionals to respond to the growing business demand for a comprehensive IT governance program that defines responsibility and accountability across the entire enterprise.

December 12th, 2009 CISA/CISM/CGEIT Exams Registration:

Early registration deadline for the December 12th, 2009 CISA/CISM/CGEIT exams is August 19, 2009 . September 23rd is the final registration deadline for the December 12th CISA, CISM and CGEIT exams. Candidates are encouraged to register online through the ISACA web site (http://www.isaca.org/) by saving $50 off of the registration fee.

Fall 2009 CISA Review Course:
The Kansas City ISACA Chapter is holding a CISA Review Course for the December 2009 CISA Exam. The course will be based on ISACA's CISA Review Manual for 2009. We recommend that CISA candidates purchase the CISA Review Manual from ISACA International (the web link for the manual is: ISACA CISA Study Guide

The sessions will be based on the recorded audio and presentation slide copies from the Spring review course. Course materials provided include a hand-out of the review presentation slides and practice quizzes with answers which will be mailed out after the participant submits the course registration form. Again, we recommend the purchase of the CISA Review Manual, separately since it is not included with our course.

The session audio is recorded and will be available for download by review participants. Along with the handouts, this would allow for self-paced study.

The registration fee for this course is $100 for Kansas City ISACA and other regional cooperative chapters' (currently Atlanta, Des Moines , Oklahoma City, Omaha and Minnesota) members and $125 for all others. Additionally, there is a mailing fee of $10 for the course materials.

The Review Course registration form can be downloaded, completed and either Emailed or ground mailed to Jerry Wistrand (Fall 2009 CISA Review Registration Form). The return address is noted on the form. The course materials will need to be ground mailed to you after the registration and payment are received. If you have any questions or concerns, please contact Jerry Wistrand at 816-760-7813 or email at g.wistrand@att.net.

CISA Certification Process:
Once you have passed the exam and have met the certification requirements (generally five years of systems audit or security experience, or allowable substitutions) as specified on the ISACA website, and then you will need to complete and submit the application for certification.

CISM Study Group Information:
No study group plans currently.

CGEIT Certification (Certified in the Governance of Enterprise IT):

ISACA's new IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. For further information, please visit the Official ISACA International website: CGEIT Certification Details.

Article: An Insider's View of Security Risk Management

Authors:

Marjorie Windelberg, Ph.D., CISM, CISSP, is Adjunct Professor in the Homeland Security Program at the Graduate School of Management and Technology, University of Maryland University College, Adelphi, Maryland 20783.

Dan Hill, CISM, CISA, CBCP, CISSP, is a Principal in the Information Assurance and Privacy practice of SRA International. He is the Director of Education and Research on the Board of the National Capital Area Chapter of ISACA.

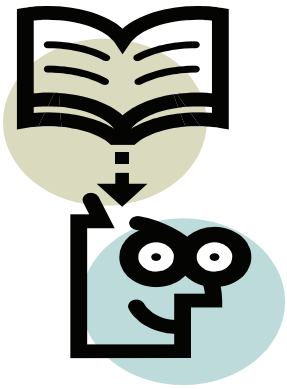
Reality Check for Risk Management

It is important to manage the expectations of others with respect to risk management. You cannot eliminate all risks. You cannot prevent every attack or incident. The reasons for this are varied. For one, resources (both people and money) are limited. For another, human attackers are determined and need find only one vulnerability to exploit, while you must defend everything. New vulnerabilities arise all the time. And it is inevitable that someone will do something accidentally or will be negligent at some time. A more realistic goal is to plan for resilience and for survivability. You should design with the goal of providing the ability to operate despite an incident -- resilience and continuity.

Different organizations also have different tolerances for risk, with some being very risk averse, and others ranging from moderately to largely tolerant of risks. The tolerance for risk need not derive from careful analysis, but may be driven by other factors such as competing priorities or even the organization's culture. An organization's tolerance for risk can also change over time, depending on events. Competition, the speed of technological change, new regulations as well as new threats can change the organization's risk profile. An incident or impending legal action can push it into being more risk averse; or, a change in senior management can increase or decrease the tolerance for risk. Thus, risk must be periodically re-evaluated.

Risk and Resilience

Richard Caralli has been researching operational resiliency in Carnegie Mellon's CERT Program. He is the lead developer of the Resiliency Engineering Framework, a process improvement model focused on managing operational resiliency. He has discovered that measuring and managing risk tolerance first requires an organization to define the boundaries of its normal operating range. These boundaries move over time, and must be periodically redefined to account for changes in the operational environment. An organization that is able to operate at the margins of those boundaries in the face of change may have a high tolerance for risk. Also, organizations with wide operating boundaries will be more resilient than those whose boundaries are narrow. A narrow operating boundary could be the result of processes with limited options available to deal with unexpected production difficulties.



A narrow operating boundary could be the result of processes with limited options available to deal with unexpected production difficulties.

We can see the relationship between operating boundaries, risk tolerance, and resilience in household operations. A household that lives from paycheck to paycheck and strives to be financially responsible has a narrow operating boundary, a low risk tolerance, and little resiliency. A family with children who are old enough and willing to help with household expenses has a wider operating boundary.

Evaluating and Controlling Risk

A big problem in quantizing risk is all the uncertainty associated with it, and uncertainty has a strong influence on managing risk. The process of decision-making includes defining events that may happen in the future, determining what information is relevant in increasing or decreasing risk, determining vulnerabilities, and estimating the impact of disruptive events.

Once existing risk levels are identified, there is more decision-making about how to deal with unacceptable risk. Because operating risk is inherent in performing business or mission functions, complete elimination of risk is impossible, short of ceasing to operate. Mitigations, also known as "controls", can be put in place to reduce operating risk to acceptable levels and increase resilience.

Strategies

The principal strategies in dealing with risk are acceptance, transference, and avoidance.

Acceptance of risk means you understand - as well as possible - the current threats, vulnerabilities and impacts of disruptive events, and the level of risk is acceptable. You have mitigations in place that are

Article: An Insider's View of Security Risk Management

reducing risk to acceptable levels, and you have enough resilience built in that you can take a hit and keep functioning at acceptable levels.

Transference of risk means another organization is willing to accept some of the consequences of a disruptive event that impacts your operation. This strategy works if there is another organization that can continue the disrupted functions at acceptable levels. If the organization is an insurance company this strategy works for financial compensation of losses.

Risk avoidance is not the same as being risk averse. If you are risk averse you have a low tolerance for risk, and want to get risk levels as low as possible. You want to do everything possible to minimize risk, through mitigation and risk transference strategies. Risk avoidance involves forgoing an activity because the risk level is too high to accept. For example, an international organization may choose to not locate to a certain country or even pull out of a country because of high levels of violence and political instability. Risk avoidance can also be personal, as when many people refused to fly after the September 11, 2001, terrorist attacks.

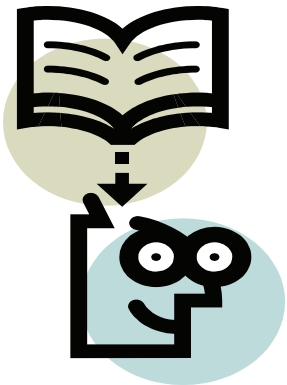
Even if you transfer some risks and accept others by choosing to mitigate them, your job is not done. You also need to evaluate the controls, both initially and periodically thereafter.

Complexities

Evaluating a control requires asking how effective it might be against the risk. Does it eliminate the risk entirely? If not, to what degree does it minimize the risk? Other evaluation questions revolve around feasibility. Are there down-sides (negative consequences or impacts) of a control? Will people accept the control or will it interfere with what they want to do? If these side-effects are not examined carefully, they result in unintended consequences.

What can be done to minimize unintended consequences of a security control? Are there resources available to implement and maintain a new control? What assurance is there that the control will work? What events could defeat the control? If the control fails, will we know it? Will it fail gracefully or suddenly and totally? Is the control isolated or inter-dependent on other controls? Does the control rely on the same infrastructure as other controls?

Also, because risks change over time, the controls may lose effectiveness or the assets being protected may become more valuable. The limits to the amount of protection afforded must be made explicit as assumptions in a business continuity plan. It is also a good idea to communicate these assumptions and the limits regularly.



In addition, options for control selection need to be evaluated as part of a larger system. A systemic and process-oriented evaluation helps to create what Sheffi calls a "layered and balanced defense," where the pieces work together to prevent complete failure if one control (or more than one control) is compromised. A systemic review should also look for possible conflicts between proposed controls. For example, federal flood control projects reduce the pressure to regulate development in flood plains.

On the other hand, some controls may mitigate the impacts of multiple threats. This relates to the all-hazards approach to emergency management. For example, hardening a building may protect against tornado-force winds as well as explosions.

Cost-Benefit Analysis

Once you have a good idea of what controls you might like to move forward with to reduce risk, the next step is to look at the costs of the controls, both start-up costs and on-going costs, or total cost of ownership (TCO). Once TCO is determined, it should be compared to the expected benefits. Once TCO is determined, it should be compared to the expected benefits.

There are several ways to evaluate costs of security controls in relation to their benefit. Lawrence Gordon and Martin Loeb have written a paper with a comprehensive analysis of various approaches. Return on Investment (ROI) is an accounting tool that looks at the past to evaluate the financial value of assets. Return on Security Investment (ROSI) also looks at the past. Internal Rate of Return (IRR) and Net Present Value (NPV) are able to look to the future and incorporate expected benefits.

Article: An Insider's View of Security Risk Management

How Much Should Security Cost?
Using a model based on NPV, Gordon and Loeb have determined that "the optimal level of investment in security-related activities should not exceed approximately one-third of the potential expected loss."

As Sheffi notes, making the business case for security is difficult, because it rests on spending money to avoid future costs. He aptly summarizes the problem: "Since costs avoided do not show up on any financial statement, or in any incentive system, and costs incurred are visible (including security outlays), there is little natural incentive to invest in cost avoidance." .

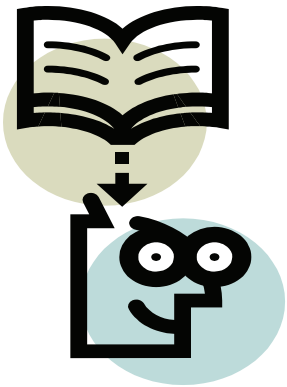
Finally, a caveat about intentional human threats. Often, the value proposition to an organization defending against low and moderate impact attacks may be less than the value to the attacker. The hidden result is that the probability of a threat becoming an event may be much higher than expected!
Security Risk Management - Process and Program

To keep operational risk under control and to keep mitigations operating effectively requires constant care. Processes help ensure consistent execution of what you know you need to do. The risk management program ensures the processes are connected with the rest of the organization, and keep working effectively.

Microsoft offers a free Security Risk Management Guide with tools and templates. The National Institute of Standards and Technology (NIST) Special Publication 800-30 “Risk management guide for information technology systems” is another source of guidance on setting up and running a security risk management program.

Change of any kind, internal and external, recognized and unrecognized, alters the risk environment. As the risk environment changes, security requirements, processes, and mitigations need to be evaluated and updated to maintain a strong security posture. Lack of focused management attention can quickly lead to disaster.

Risk management needs documented processes, and it needs a program to provide the hands-on management it needs to drive execution of the processes.



Did you know as an ISACA member, you have the opportunity to attend e-symposiums and earn CPE credits ***free of charge***?

Visit http://isaca.brighttalk.com/ to learn more about e-symposiums.

CPEs!!

Continue your education with ISACA by visiting the International ISACA website at http://www.isaca.org or the location website at http://www.isaca-kc.org

More information to come in the future newsletter with CPE options.

Upcoming Events from ISACA—International

ISACA Training Week
Presented by ISACA®, Training Week provides a unique educational experience.

The Training Week courses use a combination of lecture, case study, class discussion and group exercises to explore all the nuances and subtleties of the named topics. Training Week participants will learn about proven strategies and techniques based upon best practices and lessons learned from the ISACA community.

Network Security Conference

ISACA's Network Security Conference is uniquely designed to meet the education and training needs of the seasoned IT practitioner as well as the newcomer. Whether you are an experienced information security professional keeping pace with complex network environments, an IS auditor looking to gain detailed knowledge and competencies on specific topics, an IS control professional seeking information on guarding one of your organization's most important assets or otherwise involved with information security, this year's Network Security Conference will benefit you.

Information Security Management Conference

Strategic vision for information security managers

ISACA® is pleased to announce its fourth annual Information Security Management Conference, designed for experienced information security managers and those who have information security management responsibilities. The event will feature a variety of sessions dealing with information security managerial issues and information security programme issues. The combination of management focus and highly detailed content will provide the attendee with an opportunity to customize the conference experience to his/her specific interests and professional needs. Experienced professionals as well as new or aspiring Certified Information Security Manager® (CISM®) holders will find great value in the conference.

Visit http://www.isaca.org for more details on each event.

Feedback Forum

If you have any suggestions regarding newsletter content or formatting, please contact our Newsletter Editor,: Email: urvi.biyala@ey.com.

Bits & Pieces

Job Postings

Company	Job Title	Post Date

No posting at this time.

Visit our website for further details of each posting: http://www.isaca-kc.org/job.htm

NOTE: All job postings will be removed from the website after 90 days. For more information, please contact Pat Wallace at (913) 568-4272 or Email: patwallace001@yahoo.com .

.

2009 - 2010 Board Members

NAME	COMPANY	BOARD POSITION	EMAIL
Jim Wilcox	American Century	Director	jim_wilcox@americancentury.com
Jennifer Harper	AIPC	Director	jharper@aipc.com
Mike Connors	Doug Clark CPA	Director	connorsm@dougclarkcpa.com
Kevan Brewer	CenturyLink	President	Kevan.f.brewer@embarq.com
Jerry Wistrand	Commerce Bank	Vice President	Gerald.Wistrand@Commercebank.com
Alfie Mahmoud	KPMG	Associate Vice President	amahmoud@kpmg.com
Nila Holmquist	CenturyLink	Treasurer / CISA Review	Nila.K.Holmquist@embarq.com
Wendy Dobratz	NAIC	Secretary	wevans@naic.org
Carman Kesner	DST	Programs Committee Chair	ckesner@deloitte.com
Matt Suozzo	Protiviti	Membership	Matt.Suozzo@protiviti.com
Urvi Biyala	Ernst & Young	Newsletter Editor	Urvi.Biyala@ey.com
Pat Wallace		Job Coordinator	patwallace001@yahoo.com
Robert Seider	QLS Computer Solutions	Web Design	robert@qlsenterprises.com

ISACA Greater Kansas City | P.O. Box 26066 | Kansas City MO, 64196