@ISACA
RELEVANT, TIMELY NEWS
Volume 16, 30 July 2014

Speaker Spotlight: Company President Turned Whistle-blower to Give Keynote Address at EuroCACS/ISRM

In 2011, Michael Woodford was appointed president of Olympus Corporation. He quickly found himself to be the right man in a very wrong place when accounting fraud amounting to nearly US $2 billion came to his attention. Learn from Woodford at EuroCACS/ISRM in Barcelona, Spain, from 29 September-1 October.

Read More

Five Things Every Company Should Do to Cover Its Assets

By Mark Johnston

Data governance, i.e., having an operational strategy to maintain the integrity of an enterprise's information, is crucial. News media and web sites are filled with headlines about the latest breach of personal data or slew of stolen credit card information, meaning major corporations need to take another look at protecting customers and their data.

Read More

Earn CPE at Women in Leadership Webinar

ISACA® is offering a webinar on women in leadership, led by Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, and the Honorable Theresa M. Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA. The "Climbing the Corporate Ladder…in (Tasteful) High Heels" webinar will be held on 21 August at 12:00 p.m. EDT (UTC-04:00), and members can earn 1 CPE hour by attending.

Read More

Help Your Career and Give Back With an ISACA Certification

Thu Nguyen, CISA, CRMA, Audit Manager at Wells Fargo, Shares Her Experience as a CISA

In her role as an auditor, Thu Nguyen wanted to know how audit affected other business areas. As a result, she decided to pursue the Certified Information Systems Auditor® (CISA®) certification. "I needed to understand how the systems work as they relate to our business objectives," she says. "Early in my career, I started to ask questions about IT operations every chance I got. Then I studied for the CISA exam in hopes that it would help me understand the risk and controls behind what I do."

Read More

New COBIT-related Governance Resources Available

ISACA has issued new COBIT-related publications: *COBIT® 5 Principles: Where Did They Come From?* and *Guidance Note on Corporate Governance, ERM and Assurance for COBIT 5*.

Read More

Book Review: *Cyber Crime & Warfare: All That Matters*

Reviewed by Upesh Parekh, CISA

Cybercrime can be understood as crime committed with the aid of a computer, the Internet or both. By this definition, it could be concluded that if one is not using a computer or the Internet, one does not need to worry about cybercrime. Unfortunately, this is no longer the case.

Read More

Speaker Spotlight: Company President Turned Whistle-blower to Give Keynote Address at EuroCACS/ISRM

In 2011, Michael Woodford was appointed president of Olympus Corporation. He quickly found himself to be the right man in a very wrong place when accounting fraud amounting to nearly US $2 billion came to his attention. Learn from Woodford at the **European Computer Audit, Control and Security and Information Security and Risk Management (EuroCACS/ISRM**) Conference in Barcelona, Spain, from 29 September-1 October.

In this closing keynote speech, Woodford will discuss the Olympus Corporation scandal, his decision to expose it and the aftermath of his disclosure. Woodford and other activists are pressing the UK government to back the creation of clearly defined procedures for handling whistle-blower claims and other measures to improve corporate governance globally for all companies above a certain size. He also emphasizes the need for auditors to play a stronger role: "To become more forensic."

Unlike most whistle-blowers, Woodford was able to pay the US $1.7 million in legal expenses generated in just 12 weeks after he was fired for exposing the corporation's wrongdoing. "But what would it be like if you were a residential care worker or a junior accountant in a large organization?," he asks. "It is those people I would like to help."

Find out what the man named 2011 "Business Person of the Year" by the UK press had to go through as he fought his case—perils he hopes he can help those who expose corporate wrongdoing avoid in the future. Learn more about Woodford's speech and the other sessions on the **EuroCACS/ISRM** page of the ISACA web site.

Five Things Every Company Should Do to Cover Its Assets

By Mark Johnston

Data governance, i.e., having an operational strategy to maintain the integrity of an enterprise's information, is crucial. News media and web sites are filled with headlines about the latest breach of personal data or slew of stolen credit card information, meaning major corporations need to take another look at protecting customers and their data.

There are 5 steps every enterprise needs to take to govern its data more effectively:

1. **Access controls**—Imagine an employee being fired or relocated but still having full access to every bit of information he/she had as an employee. The quality of a company's data hinges on its limited access to trusted internal staff for management and oversight. When turnover occurs within a business, controls enable a company to anticipate changing permissions to maintain access to private information. Implementing access controls will establish continuous monitoring of employee accounts, automatically alerting executives when a violation occurs, and ensuring a disgruntled former employee cannot log in and potentially steal or alter data.
2. **Segregation of duties**—Make sure there is more than 1 person involved in sensitive processes or business duties that could lead to fraudulent behavior. For example, the person who approves expenses in payroll should not also be the person writing all the checks. Ensuring an enterprise reconciles databases and actual activity will help guarantee segregation of duties (SoD) compliance, alerting executives to high-risk conditions.
3. **Critical data governance**—Think of how many critical, sensitive and important documents exist within an organization. Governing that information is a top priority for businesses and overseeing it with proper controls can safeguard it as it moves throughout the enterprise. Critical data controls can alert business leaders when a confidential document is inappropriately released, in addition to scanning documents for sensitive customer information. The same controls can ensure data quality for incoming and outgoing critical data while masking delicate fields to adhere to industry privacy standards. Furthermore, software can track data flows, watching the path sensitive data take as they move around the organization.
4. **Log and event governance**—While many major enterprises have security measures in place to alert them to potential errors, sometimes the number of notifications can be incredibly overwhelming. Log management aggregates and prioritizes data from multiple sources, consolidating important information so teams can take action in critical events without having to weed through the clutter. The software can also trend and analyze the log of events, taking a closer look at any correlation between issues.

5. **Suspicious activity**—Theft, fraud, misuse and more—it is all classified under suspicious activity. New data controls can automatically monitor and alert executives to potential employee fraud, waste and abuse. For example, if a company's fleet of vehicles normally drives 300 miles per week and suddenly that number jumps to 600 miles, software controls will flag the suspicious activity. The controls can also track vendor invoices, expense reports, payments and accounts payable for cases of fraud.

Using data controls in new ways streamlines business, saves time and helps ensure accuracy. Controls can also be used to monitor and protect your organization from fraud, unauthorized access and more.

Internal threats lurking beneath the surface can impact business even as companies fear external intrusion. These tips provide companies with practices to ensure data maintain a rigorous level of integrity at each interaction, starting at the core of a company's data input.

Mark Johnston is the product adoption manager at Infogix, Inc. He works with companies in the financial services, insurance, telecommunications, health care and retail industries.

Earn CPE at Women in Leadership Webinar

ISACA® is offering a webinar on women in leadership, led by Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, and the Honorable Theresa M. Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA. The "Climbing the Corporate Ladder…in (Tasteful) High Heels" webinar will be held on 21 August at 12:00 p.m. EDT (UTC-04:00), and members can earn 1 continuing professional education (CPE) hour by attending.

The webinar will include advice on becoming a trusted advisor, being influential, and creating and building a personal brand. Stewart-Rattray and Grafenstine will also share information on what they wish they had known 20 years ago. The webinar will conclude with an opportunity for attendees to ask questions.

Stewart-Rattray is the first woman to serve as chief information officer responsible for both operational control systems and business systems in the utility sector in Australia. Grafenstine is the first woman to serve as the inspector general of the US House of Representatives.

To register for this webinar or to learn more about it, visit the **Climbing the Corporate Ladder…in (Tasteful) High Heels** page of the ISACA web site.

Help Your Career and Give Back With an ISACA Certification

Thu Nguyen, CISA, CRMA, Audit Manager at Wells Fargo, Shares Her Experience as a CISA

In her role as an auditor, Thu Nguyen wanted to know how audit affected other business areas. As a result, she decided to pursue the Certified Information Systems Auditor® (CISA®) certification. “I needed to understand how the systems work as they relate to our business objectives,” she says. “Early in my career, I started to ask questions about IT operations every chance I got. Then I studied for the CISA exam in hopes that it would help me understand the risk and controls behind what I do.”

In addition to helping her better understand business operations, the CISA certification has also provided Nguyen with a networking resource. “As a CISA, you belong to a well-respected worldwide professional organization that continuously supports your professional aspirations,” she says. “Sharing knowledge, giving back to the profession and being informed is the best part of being a CISA.”

But for Nguyen, the CISA certification does more than just help her career; it enables her to give back to the community. “I am able to give back to the profession in so many ways. I joined my local ISACA® chapter as a leader and director to support our mission,” she says. “I lectured and taught at various colleges and universities to help open young people’s minds and eyes to the possibilities of a career in IT audit, security, compliance and so many more opportunities of which the students had not thought. I am a mentor to many aspiring professionals in my work and private life.”

And to those considering a CISA certification, Nguyen advises, “Do it! It will only enhance your career aspirations and open doors in so many aspects of your professional life.”

To learn more about certification, visit the **Certification** page of the ISACA web site and join the **CISA (Official)** group on LinkedIn.

New COBIT-related Governance Resources Available

In support of COBIT® 5, ISACA® has issued two new publications:

- ***COBIT 5 Principles: Where Did They Come From?***—Governance and management of enterprise IT (GEIT) is the board's accountability and responsibility, and the execution of the set direction is management's accountability and responsibility. COBIT 5 is primarily a framework made by and for practitioners. It includes insights from IT and general management literature, including concepts and models such as strategic alignment, the balanced scorecard, IT savviness and organizational systems. By clearly indicating how the principles of COBIT 5 are built on these IT and general management insights, this white paper helps practitioners to understand COBIT 5 principles and, therefore, be more efficient and effective in their endeavors to apply COBIT 5 in their organizations.
- ***Guidance Note on Corporate Governance, ERM and Assurance for COBIT 5***—Section 211 (7) of the Indian Companies Act, 1956, requires reasonable steps to secure compliance. The new Companies Act, 2013, has many of the previous requirements and adds a number of corporate governance and risk management requirements. The focus of this white paper is to use COBIT 5 to guide the board, management and auditors in complying with requirements arising from Clause 49 of the Securities and Exchange Board of India's (SEBI) Listing Agreement and the new Companies Act, 2013.

Additional information on recent and upcoming research projects is posted on the **Current Projects** page.

Book Review: *Cyber Crime & Warfare: All That Matters*

Reviewed by Upesh Parekh, CISA

Cybercrime can be understood as crime committed with the aid of a computer, the Internet or both. By this definition, it could be concluded that if one is not using a computer or the Internet, one does not need to worry about cybercrime. Unfortunately, this is no longer the case. *Cyber Crime & Warfare: All That Matters* cites an incident in which a newly built water supply and sewage system was forced to shut down by a cyberperpetrator who was using a laptop and wireless equipment. With increasing dependence on computers and the Internet, cybercrime is

an area of concern and curiosity for many people, notwithstanding their technical fascination or capability.

However, many people are afraid of technical jargon and complexities when reading about cybercrimes. *Cyber Crime & Warfare: All That Matters* is written for general readers and students who want to gain preliminary insight into cybercrime. The book is devoid of technical jargon and complexities and is appropriate for those who want to get a firsthand understanding of cybercrime.

This brief book highlights many subtleties of cybercrime with real-life examples and anecdotes. Being careful not to require too much technical knowledge of a casual reader, this book explains uncommon terms in simple language. The book covers viruses, hacking, identity theft, cyberwarfare and more.

Technology is a double-edged sword. The cyberfuture is promising, bewildering and a bit horrific. This book will help unravel some of the mysteries behind cybercrime.

Cyber Crime & Warfare: All That Matters 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.