ISACA®
Trust in, and value from, information systems
Denver Chapter
Volume 10, Issue 3
April 11, 2012

Name our Newsletter!!! See details below

INSIDE THIS ISSUE:

Win $100 gift card

Help name the Newsletter and you could win $100 gift card. We are looking for a new name for the ISACA Denver Chapter Newsletter. All you have to do is submit a new newsletter title and if you entry is picked you will win a $100 gift card to Amazon. All entries must be submitted by May 1, 2012 to be considered eligible for the prize. Submission should be sent to secretary@isaca-denver.org

ISACA Denver Chapter' Annual General Meeting

April 19, 2012 | 11:00 AM to 4:30 PM
Social To Be Held Afterward

Ron Ross, PhD will present "A Risk Management Framework to Improve Information Security and Strengthen Risk Management". To learn more about the presentation, and to register, please go to the chapter's website at http://isaca-denver.org/Chapter-Meetings/April-Chapter-Meeting.php.

Please note: ISACA Denver will be holding their elections for 2012/2013 Board Positions at the Annual General Meeting, therefore member attendance is strongly encouraged.

Please note, voting for board positions will also be done on-line this year. On-line voting will start on April 13th and go through April 17th. Watch for your on-line invitation in your email.

COBIT 5 is here!!

COBIT 5 is the latest edition of ISACA's globally accepted framework. The most significant evolution in the framework's 16-year history, COBIT 5 now provides an end-to-end business view of the governance of enterprise IT that reflects the central role of both information and technology in creating value for enterprises. The principles, practices, analytical tools and models found in COBIT 5 embody thought leadership and guidance from business and IT leaders and governance experts from around the world. https://www.isaca.org/COBIT/Pages/default.aspx

Get to know your board members

This month we highlight Rhonda Willert, the ISACA Denver Academic Relations Coordinator

Rhonda Willert, is a Senior Manager with Deloitte in the Audit and Enterprise Risk Services, Advisory Group. Rhonda has been with Deloitte for 7 years, prior to Deloitte she worked in the telecommunications industry at AVAYA, Inc. At Deloitte she focuses on energy and federal clients and assists with financial transformation projects to improve business operations (both financial and operational). Rhonda also supports the IT and business process controls auditing on Deloitte audit clients.

Rhonda graduated with a master's degree in Accounting from DU, and got her undergraduate, a bachelor of science with an emphasis in IT/Accounting/and Finance at CU. Rhonda holds certifications as a CPA, CISA, and PMP. Please feel free to reach out to her with any questions you may have in relation to ISACA, Public Accounting, Certifications, or other topics, as she is always willing to discuss these areas.

Rhonda is the ISACA Denver Academic Relations Coordinator, and has been for the prior 6 years. She has significantly grown this community service which now serves many of the state of Colorado's major collegiate institutions. The Academic Relations Committee provides Colorado students networking and educational opportunities around the field of auditing and security and holds an annual scholarship contest for Colorado students; this year's winners' submissions can be found in this month's newsletter.

ISACA's Academic Advocate Program

As an influential member of your academic institution's faculty, you value the education your students receive and the direction it gives them in choosing a professional career. ISACA® partners with its Academic Advocates, to encourage students to prepare themselves for satisfying careers in information systems assurance and control, risk, security and governance of enterprise IT. By becoming an ISACA Academic Advocate, you will gain access to an abundance of resources to assist your students and to benefit you as well.

Academic Relations Update

By Rhonda Willert, ISACA Academic Relations Chairperson

This year has been a year filled with change for the Academic Relations committee. Over the past few years, we have experienced growth with the amount of volunteers, therefore, attempted a committee restructuring effort this year. This restructuring allowed our volunteers to focus on specific areas of the academic relations program: Specific University programs, Scholarship Program, Academic Advocates, Student Sponsorship/Mentoring Program, and Student Group efforts.

This year we have presented about ISACA to students at the University of Colorado at Denver, Metropolitan State College of Denver, Denver University, Pikes Peak Community College and University of Colorado at Boulder. We hope to complete a few more before this fiscal year ends. We also will hold our first student group event on Thursday April 12th!

I want to thank our lead volunteers by area including: Jaimie Sylman for Scholarship program and for the University of Denver efforts, Mary Bloomingdale for the Sponsorship Program, Scott Murphy & Channa North-Hoffstaed for the Student Group Program, Josh Ladner for Metropolitan State College of Denver efforts, Aaron Wilton for Colorado State University efforts, Jennie Johnson for University of Colorado at Boulder efforts, Alex Bitti for Regis University efforts, and Richard Allen for University of Colorado at Colorado Springs and Pikes Peak Community College efforts. Without these individuals assistance, we could not have accomplished all that we did this year. I also would like to thank our additional volunteers assisting with all areas of the academic relations program including volunteering for the school presentations, contacting students and professors, and many other activities to support our initiative: Dustin Palmer, Jordan Deherrera, Roger Bland, Ashley Beste, Christina Pagano, Marc Trevino, Ben Pepper, Sarah Davis, Mara Angenendt, Geneva Debarros, Collette Thepenier, Connie Spinelli, Anja Norman, Matthew Sharp, Jennifer Ware, Jon Pitts, and Maria Hao.

Last year the academic relations committee established a “sponsor program” where volunteers meet with the students that are attending our ISACA professional meetings. These “sponsors” met the students at the registration table and introduced the students to fellow ISACA members, helped them to feel comfortable attending our professional events, and also helped them to see the benefits of being involved with professional organizations such as ISACA. This program continued into this year, and we hope will expand even more in the future. The students have commented that this is an excellent process and made them feel comfortable at the meetings and more likely to attend additional meetings. I would like to also thank our sponsorship volunteers who remained on call for these students: Ben Pepper, Christina Pagano, Jennie Johnson, Meenal Mukadam, and Jon Pitts. This year our Academic Advocate, Jim Marlatt, brought several students from his classes at the University of Colorado at Boulder to a few of our ISACA meetings, and we also had two university students, one from DU and one from Texas A&M who attended with interest.

Our first official ISACA student group event will be held on Thursday April 12 this year, led by Scott Murphy & Channa North-Hoffstaed. This will be a student event for both active student members and non-members. The event will be a great way for the students to network with professionals who volunteered to attend, and gain insight into the benefits of ISACA membership as a student and business professional. The evening events will include; Networking with ISACA members and Students, Guest Speakers, Scholarship and Membership Opportunities, light appetizers, and prizes. Thank you to our speakers: Jon Pitts, Mark Gengozian, Channa North-Hoffstaed, and the Networking volunteers: Brennan Baybeck, Matt Randolph, Ram Ramadoss, Jim Marlatt and Scott Peyton.

Our team attended a Certification Night hosted by the Metropolitan State College of Denver’s Accounting Student Organization (ASO), led by Josh Ladner with the assistance of Jordan Deherrera to discuss the different certifications that ISACA has to offer. It allowed ISACA to gain one on one time to speak with the students and teachers about the different opportunities ISACA provides to professionals and the alternative career paths in the IT Audit field for students with Accounting and Information Systems backgrounds. Students and teachers were able (and encouraged) to approach the booth that was setup for ISACA. Our professional representatives provided a high level overview of the organization and our mission, answered questions about joining ISACA, and obtaining certifications. Other professional organizations that attended the event included Colorado Society of CPA’s, Institute of Internal Auditors, Associated of Certified Fraud Examiners, and several others. The event resulted in an increased knowledge of ISACA at the campus for students and teachers alike, and sparked interest in future ISACA participation whether it is a presentation in a classroom or attending an ISACA professional event.

Our program also held one large event at the University of Colorado at Boulder – Leeds School of Business , led by Jennie Johnson with the assistance of Jim Marlatt. The purpose of this event was to provide students of the CU Boulder AIS (Accounting Information Systems) and Beta Alpha Psi (Accounting, Finance and Information Systems) groups with an opportunity to meet, learn from, and network with ISACA professionals in various industries (i.e., to learn of different career paths ISACA members have taken and how the various certifications offered by ISACA have helped them advance or pursue new directions in their professional lives). This event was a huge success in which we had over 50 students attend. A big thank you to our speakers: Steve Fox, Suzanne Straub, Jon Pitts, Emilie Spear, and Mary Bloomingdale; and also a big thank you to our networking volunteers: Anja Norman, Grace Roberts, Don Mapes, and Rob Ellis.

I also want to thank our Academic Advocates Jim Marlatt, University of Colorado at Boulder, Dan Likarish, Regis University, and Kris Brands, Regis University and our newest academic advocate - Ms. Barbara Uliss, Metropolitan State College of Denver (Welcome!). We assisted Dan at Regis this year as he put on the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC). The competition was open to all community, junior, bachelorette and university schools for the Regional competition that allowed them to advance to the National event in San Antonio. This event was a success, and we were glad to support one of our advocates with their initiative, and provide ISACA members who volunteered CPE credit.

For some additional background, the Academic Advocate Program was developed to assist educators in preparing students for rewarding careers in the information systems assurance, control risk and security, and enterprise governance professions. The Academic Advocate program works to enrich students’ careers, enhance professional resources, and grow the profession.

There are many benefits to becoming an Academic Advocate, including but not limited to:

- ISACA membership is complimentary to all Academic Advocates and provides additional benefits including: access to ISACA’s eLibrary, an ISACA Bookstore discount, subscription to the ISACA® Journal and much more.
- ISACA Model Curriculum for IS Audit and Control and ISACA Model Curriculum for Information Security Management.
- CobiT®. A hard copy of CobiT is supplied to Academic Advocates. CobiT helps organizations develop an internal IT control system that supports business processes in four domains: plan and organize, acquire and implement, deliver and support, and monitor and evaluate.
- ISACA eLibrary is a comprehensive, on-demand collection of content from nearly all ISACA/IT Governance Institute published books and over 250 additional titles—all available free of charge to Academic Advocates.
- Academic research is a vital part of any curriculum. Academic Advocates and their Ph.D. students can submit research surveys for evaluation and possible posting to the ISACA web site.

We are looking for more academic advocates to represent ISACA at other Colorado universities. Right now we have Metropolitan State College of Denver, Regis University and University of Colorado at Boulder represented, but we would like to expand our reach to additional schools. To find out more about being an academic advocate visit www.isaca.org/academicadvocate .

Please see our Scholarship Program Update starting on page 6

Challenges in getting ITG off the ground, By Koushik Kumaraswamy CGEIT

In the previous couple of articles in the IT Governance corner, we have covered the definition as well as the need for IT Governance. Unfortunately, knowing "that what & the why" of IT governance, does not make it any easier to implement it successfully – i.e. "the how". This is exactly where several organizations find themselves - wanting to proceed with ITG but struggling with the process of implementation. We explore some of the challenges of ITG implementation in greater detail in this article.

General Misinformation: A simple Google-search on "IT governance frameworks" returns quite a few articles with references of various frameworks mentioned including ITIL, Six Sigma, PRINCE2, etc. A lot of this information is plain wrong! For e.g. Scope addressed by ITIL would be Service Management – not IT Governance, PRINCE 2 addresses Project / program management and Six Sigma for process improvement and control. None of these frameworks provide explicit top level guidance on how to make IT support and extend enterprise goals. With this much misinformation around the definition, the organization (outside the core implementation team) has varying ideas about what ITG is and have diverging expectations from the initiative as a result. This "noisy" background environment is a major roadblock for ITG implementation wherein involved stakeholders don't quite understand the initiative in the first place and are unable to align themselves behind it. A key takeaway here is to incorporate a clear communication & education program to prepare the organization for the change wrought by ITG.

Cart leading the horse: Informed CIOs that understand the value of ITG push for its implementation within the enterprise. In a lot of cases, they end up owning the initiative within the organization. This is of course contrary to the spirit of ITG wherein the goal is to elevate key decision processes to the senior leadership of the Business. This intermixing of governance and management leads to dilution of ITG and it often devolves into an "IT improvement initiative". The takeaway here is for ITG champions to sell the benefits of ITG to the business leadership in the context their current priorities and issues. The leadership team needs to be able to make a clear connection between ITG implementation and the solution to their current priorities. The goal at that point would be to build in a virtuous cycle where positive implementation results would reinforce support for the ITG process and thus, make it a part of the enterprise DNA.

Complexity: ITG is a discipline that covers several domains and competencies. Its pervasive scope makes its implementation inherently complex. Key decisions involve making trade-offs between very important alternatives and require significant changes to status-quo. A very common scenario is when a decision is taken to centralize IT projects approval & funding. The idea here is to presumably prioritize and selective fund IT projects based on a corporate investment criteria (central to the portfolio management approach). While this is a best-practice approach, it might inadvertently introduce latency into decision process for intra-department or intra-business unit projects. When the individual units had the discretionary spend authority, they would have decided on their projects way more quickly compared to the time it would now take to navigate the corporate investment process. So the trade-off here is between investment outcomes and agility – not a binary situation. An ITG implementation has to persist through many such tough calls. Complete leadership engagement can help steer an implementation through such situations in a fashion that is germane to the enterprise.

Approach philosophy: Several ITG consultants that assist in implementation initiatives come to the table with the goal of implementing a framework. This line of thinking generates a lot of activity aimed at framework compliance as an end. Not good! The goal should always be to achieve the outcomes that ITG enables and never to implement a framework (even if it is COBIT!). The role of a framework is to guide the enterprise on the journey to reach its desired outcomes – i.e. it is the vehicle and not the destination. A critical success factor is the wisdom to tailor available frameworks to the constraints and realities of an organization and then use it as a powerful tool to help achieve end goals.

The issues mentioned above are just a few of the major roadblocks that need to be addressed as an organization go through an ITG process implementation. But help is in sight! COBIT 5 is coming out shortly and is set to provide a lot of detailed guidance on this topic. We will continue to explore the evolution of this discipline as COBIT 5 is released and adopted by the Industry.

If you would like to share any challenges that you have faced in your organization during ITG implementation, please use the comment feature on the blog http://governingit.blogspot.com to get back to us.

New! Volunteer Information Center

As an ISACA member, you belong to a community of professionals that share mutual goals, interests and commitments. Becoming involved with your Denver chapter will allow you to make valuable connections with peers, share knowledge and discover new opportunities in your profession. Have you ever considered volunteering a few hours of your time to the Denver ISACA chapter? It's a great way to connect with other ISACA members, local companies and your community. It's also a great way to earn CPE credits and attend the annual dinner for volunteers.

Volunteer opportunities can range from one-time tasks or committee involvement, to chapter board leadership roles including chapter president. Some examples are helping out at the CISA, CISM, CGEIT and CRISC certification training classes and taking part in the next Rocky Mountain Information Security Conference (RMISC).

A new Denver Chapter Volunteer Information Center webpage is coming soon. Watch for it at http://isaca-denver.org/. Visit this page for current volunteer opportunities, feedback from the volunteers, news about the 'volunteer of the month', and much more!

Reasons Members Volunteer:

- Give back to their profession
- Gain recognition as an influencer or expert in the professional community
- Share and gain knowledge
- Networking and personal growth

Volunteers and their employers benefit from increased self confidence, broadened professional expertise, enhanced leadership and decision-making skills, and an extensive network of professional colleagues that comes from this opportunity.

Join us in shaping your profession, as well as your future, as an ISACA volunteer.

Contact information

Contact your volunteer coordinators, Judy Bell and Terry Paulson, anytime at Volunteers@isaca-denver.org

CISA, CISM, CGEIT

June 2012 Exam-prep Group Study Sessions are Gearing Up!

- CISA, CISM and CGEIT Study Sessions prepare ISACA Denver Chapter Members for the June 9, 2012 Certification Exams.

- Five (5) CISA, CISM, CGEIT Study Sessions are planned:
  - Starting on Saturday, April 28th, 2012
  - Start time: 09:00a to 1:00p (length - 4 hours)
  - Saturday mornings on these dates:
    1.) April 28th
    2.) May 5th
    3.) May 12th
    4.) May 19th
    5.) June 2nd

- Location – Deloitte LLP, 555 17th Street, Suite 3500 (35th floor) Denver, CO 80202 (Meet in the Lobby by the Security Desk)

- All attendees must be in the Lobby no later than 8:50am on Saturday mornings. Elevators are secured from normal access, so, a Deloitte representative will be required to use their pass to transport the CISA and CISM attendees and mentors to the 35th floor.

- Attendees:
  - Agendas and general information will be distributed to all attendees prior to the first session.
  - Sign-up for Attendees is available anytime. Contact the Certification Coordinator listed below.

- Mentors/Facilitators:
  - Volunteers for Committee & Mentors/Facilitators positions are being finalized.
  - Do you wish to volunteer? Contact the Certification Coordinator listed below.
  - CPE's can be earned – 1 CPE per hour; maximum of 20 CPE's per year earned on these committees.
  - We have received a lot of interest, but, are looking to assist more of our membership, so please contact us today!

Thank you and look forward to seeing you at the sessions.

Certification Committee Coordinators:

CISA - Mark Gengozian	markge@ix.netcom.com	303-807-2877
CISM - David Vos	david.a.vos@hotmail.com	303-204-0837
CGEIT – Koushik Kumaraswamy	koushik.kumaraswamy@gmail.com	303-810-6719

ISACA®
Trust in, and value from, information systems
Denver Chapter

Scholarship Program Update

For the eighth year in a row, ISACA's Denver Chapter sponsored a scholarship program available to students attending accredited universities throughout Colorado. This year we changed the scholarship program to offer it to more students by presenting at an increased number of colleges across Colorado and offering additional subject topics.

The topics that students could use to prepare a 2-3 page essay were as follows:

- IT Governance (e.g., how IBM's Smarter Planet Initiative effectively utilizes information technology to advance strategic goals for the company)
- IT Assurance (e.g., the importance of IT Assurance Services for outsourced IT services business models like Apptis, Inc.)
- IT Security (e.g., security issues surrounding the utilization of cloud computing)
- IT Risk Management (e.g., Integration of IT Risk Management with Enterprise Risk Management)

We provided six scholarship awards, two awards at $1,500, two awards at $1,000, and two awards of $500. With this new expanded program, offered to the students in Colorado, we received essays from the following schools: University of Colorado at Denver, University of Colorado at Boulder, Regis University, Metropolitan State College of Denver, University of Denver, and University of Colorado at Colorado Springs.

We have completed our selection process and are pleased to announce the following recipients:

- Daniel Jenson, University of Colorado - $1500
- Jacky Song, University of Denver - $1500
- Sheila Swan, Metropolitan State College of Denver - $1000
- Junior Bernadin, Regis University - $1000
- Yulin Wang, University of Denver - $500
- Kyle Torres, University of Colorado - $500

Most of these students will attend the April ISACA meeting to receive their checks, please be sure to congratulate them! The winning essays are published in this newsletter below.

I would like to thank the team of ISACA members that helped review, evaluate, and select the winners from the pool of applicants. This program could not have been possible without their help: Jaimie Sylman, Roger Bland, Matthew Sharp, Suzanne Straub, Aaron Wilton, Mara Angenendt, Ashley Beste, and Geneva Debarros. In addition, I would like to thank Rose Olveda, Scott Peyton, and Tim McCain for their additional help with sending out communications about our scholarship program via email, Twitter, Facebook, the ISACA Newsletter, and maintaining the scholarship web page.

Finally, thanks to the membership for supporting this important program. Through our scholarship program we continue to improve our reach into the universities throughout Colorado and increase awareness of the field and ISACA.

Daniel Jenson Essay:

IT Security in the Mobile Workspace or Problems with Wireless and Integrated Devices

Anything that is connected to a network can be hacked. That's the statement I used to preface a lecture to some of my less tech-savvy relatives, warning them of the vulnerabilities resident in many convenient devices and applications. I am certainly no expert on information technology (IT) security, but I know enough to know what I do not know, and the possibilities are unnerving. As a high school student, I engaged in a casual competition with some friends to see who could be the first to access a protected school district database, and although I have no real hacking skills I succeeded by finding a backdoor through the default email application. I am happy to report that I did not exploit that access to modify my grades or cause any kind of mischief, nor did I continue a career as a cyber-criminal. I am sorry to say, however, that I have not kept up with advancements in IT administration or security—once a Novell Certified Network Administrator, my credentials have long been out of date. Although I do not comprehend the full depth of modern security solutions and related risks, I recognize that if an untrained teenager ten years ago was able to find a way in, it cannot be very difficult for a determined and potentially ill-intentioned intruder today.

Security has always been a challenge of information systems. It seems like security solutions are often trying to catch up with the latest threat rather than staying ahead of the curve. Perhaps one reason for this is that the underlying architecture on which IT systems are based was not designed with security as a primary consideration. The multitude of physical and logical paths by which information may be transmitted over a network between the same two points is fundamental to the availability and integrity of information systems, but it is also representative of inherent susceptibility. The IT objectives of confidentiality and availability sometimes seem in conflict with each other, and while both is essential, product development tends to disproportionately emphasize availability. This troubling trend is undoubtedly a natural response to consumer appetite for faster, easier access to anything, anytime, anywhere. Nowhere is it more evident than in the mobile device market.

The draw of wireless communication and information systems is undeniable. The constraints imposed by reliance on a wired device feel foreign to the instinctively independent human psyche. Add the convenience of mobility with the lucrative savings of switching from a commodity-based, infrastructure-intensive network solution, and it is no wonder that individuals and enterprises alike are jumping on the wireless bandwagon. Admittedly, from a cost and performance standpoint, wireless access points connected by fiber optic trunks are probably the way of the future. Smartphones are not going away any time soon, and recognizing the growing demand for airborne broadband, the International Telecommunications Union's recent World Radio communication Conference approved two new technologies implementing the International Mobile Telecommunications-Advanced standard and moved towards allocating additional radio frequency spectrum to mobile broadband services. These and other technological developments will accelerate the widespread adoption of wireless networking with accompanying security challenges for which the IT industry at large may not be fully prepared.

Before discussing wireless security more specifically, a couple of examples may serve to demonstrate the dangers of cutting-edge IT.

Researchers at Carnegie Mellon University developed a DARPA-funded application called PittPatt that compares facial features in a captured image with millions of online images, recognizing matches. If enough relevant information can be found on the internet, this software could enable the identification of a random person from a single picture. One of the researchers took it a step further, creating an iPhone app that first utilizes PittPatt to identify a person and then performs additional data extraction from publicly accessible websites to predict that person's Social Security Number. While not 100% accurate, the results were nevertheless alarming. Fortunately, this technology is not yet commonly available, but it is only a matter of time before Google, which purchased PittPatt, releases it in some form.

Another technology that has received some attention in the news because of the risk it poses is geotagging – the practice of embedding GPS-derived location information as metadata in pictures and other media generated by a smartphone. Many users are unaware that geotagging occurs, but when they post their pictures to a social networking site, the metadata often remains accessible and their position can be ascertained. This capability is a stalker's dream come true and also empowers other activities such as profiling and social engineering. Twitter has introduced a geotagging feature, but it is wisely disabled by default.

While these examples relate more directly to privacy concerns than wireless security, they illustrate the opportunities opened to criminals by what are intended to be useful innovations.

Change, even for the better, creates liabilities.

IT security has come a long way in the relatively short time that it has received serious attention. Standards and best practices are implemented to guarantee the maximum possible protection of digital resources while permitting access to authorized individuals. Wireless networking puts a wrinkle in some of those plans. For instance, a common enterprise approach has been centralized management and administration of IT resources, where workstations remain connected to the corporate network at all times, allowing the computer administrator—an IT professional—to control configurations and perform security updates. Interoffice network traffic could be easily segregated from external communications by a robust firewall, minimizing gaps in the virtual fence. The challenge and risk of provisioning a secure connection to a personal workstation at home via a Virtual Private Network (by no means a new development) is compounded when the personal workstation is a laptop, tablet, or smartphone which may be anywhere in the world, certainly not under the control of a central administrator. As the variety of supported platforms and connection methods increases, so does the required complexity of logical controls and correspondingly the susceptibility to compromise. Physical controls for wireless networks are practically nonexistent.

The most obvious security concern of wireless communications is the potential that transmissions will be intercepted. Although there is an opportunity for interception in physical media, the mechanisms are more complicated and the intrusion more noticeable than with wireless. Wireless devices typically broadcast indiscriminately in all directions, and broadcast frequencies are stipulated by law, making it very easy for a third party to collect the signal.

Exploiting the signal may be more difficult, especially with advanced encryption techniques, but public Wi-Fi networks are usually unencrypted, and foreign wireless communications are notoriously insecure. Intercepted transmissions can expose passwords, account numbers, and other sensitive information. At the other end of the link is an open receiver waiting for a signal, presenting other worrisome possibilities.

Conventional perceptions of information system boundaries are being erased both by traditional IT resources becoming more mobile and also by historically stand-alone systems becoming networkable. Television commercials advertise the ability to control home thermostats, turn lights on and off, and even start a car remotely using a smartphone. General

Motor's OnStar touts a service they call "Stolen Vehicle Slowdown," which remotely controls a car's speed. Security concerns have led to the formation of a research group called the Center for Automotive Embedded Systems Security, which proved the possibility of illicitly taking control of critical components through wireless access points. Future IT security solutions will need to address integrated wireless devices in an assortment of non-typical carriers.

Certainly none of what I have said is news to professionals in the IT security industry, who have probably been working for many years already to remedy the risks I have enumerated. I am afraid that often their efforts are underappreciated, partly because their most successful results are transparent to the average user. Security breaches are energetically publicized while preemptively thwarted attempts receive no recognition. Nevertheless, as information systems become more embedded in our lives and society's reliance on IT services increases, the need for viable security solutions will only become greater. The accelerating proliferation of wireless networks and integrated devices along with unforeseen advancements will produce some growing pains, and the industry may never really get out in front. Regardless, I am confident that digital anarchy will be averted through the unceasing efforts of people who know what I do not.

Jacky Song Essay:

Implementation of IT Governance: Macro and Micro

With the rapid development of the information technology, organizations become increasingly dependent on their information systems. Every organization, whether large, small, public, or private, need a way to ensure that the IT function complies with the organization's strategies and objectives. IT governance has become the difference between success and failure in today's high-tech environment. Critical dependency on information technology calls for a specific focus on IT governance to ensure that the investments in IT will generate the required business value and that risks associated with IT are mitigated (Hamidovic, 2010, Page 1). However, in the process of implementation of IT governance, companies often overlook two critical aspects – the macro and the micro implementation, which leads to the inefficiency and ineffectiveness of IT governance. The macro and the micro aspects can be further divided into two different levels: national culture versus corporate culture and overall success versus partial success.

National Culture versus Corporate Culture

Corporate governance is "the set of processes, customs, policies, laws, management practices and institutions affecting the way an entity is controlled and managed" (Brisebois, Boyd, Shadid, 2008, Page 31). As a subset discipline of Corporate Governance, IT governance is also highly correlated with the macro environment – the culture. Therefore, the IT governance of Coca-Cola China would be different from that of Coca-Cola US; the IT governance of Google would be different from that of GE. Being aware of the national and corporate cultural differences is key to the successful implementation of IT governance.

Compared to business groups consisting mainly of domestic companies, many global companies with significant international presence often find it difficult to manage their global IT operations. The major barrier is the diversified cultures which include language, local customs and regulations, value systems, and working styles. All of these contribute to the difficulty of IT governance in a global environment.

"In China, the daily conversation may or may not be in Standard Mandarin and the average employees may still need security awareness training to prevent them from disclosing confidential data. In Europe, one's Greek colleague might not understand English, and in south Asia, workers may rely on the slower dial-up phone line as a main access route to the Internet. Time differences prevent the corporate headquarters from setting up a video conference that would be better than not communicating at all, but still less effective than a face-to-face meeting." (Uehara, 2010, Page 1).

These issues cannot be adequately addressed by a static model of IT governance. Global business groups should try to localize their IT governance based on the local culture in which their international branches are located. A simple copy of the IT governance in the headquarters will not work as efficiently and effectively in a different country. Also, Corporations cannot expect to extrapolate or borrow a strategy from another company. What works strategically for one organization may not have the same impact on another organization. Since IT governance is affected by a company's unique culture and working practices, it should reflect the company's own goals and ambitions.

The traditional "payment and sanction" governance style to manage IT staff/users and control their activities has become less effective. Many global businesses cannot afford to allocate sufficient resources, whether internal or external (outsourcing), to IT management to spread into their worldwide business units. "In this global IT governance era with the worldwide economic downturn, hard IT governance, as typified by payment and sanction, is inadequate to manage a business's IT effectively and efficiently." (Uehara, 2010, Page 1). "To complement and enhance global IT governance, the new concept of soft IT governance can be applied by applying Soft Power theory. Joseph Nye, the author of Soft Power: The Means to Success in World Politics, and the advocate of the Soft Power theory, defines the basic concept of power as: The ability to influence others to get them to do what you want. There are three major ways to do that: one is to threaten them with sticks; the second is to pay them with carrots; the third is to attract them or co-opt them, so that they want what you want. If you can get others to be attracted, to want what you want, it costs you much less in carrots and sticks.

Thus, he coined the term soft power to: Describe a nation's ability to attract and persuade. Whereas hard power - the ability to coerce - grows out of a country's military or economic might, soft power arises from the attractiveness of its culture, political ideals, and policies." (Uehara, 2010, Page 1).

Inferred from the Soft Power theory, Soft IT governance should become a useful IT management tool to support business. It gives corporations the flexibility and adaptability when implementing IT governance in different national cultures and corporate cultures. In reference to CobiT's 34 processes, the hard and soft IT governance can be combined to realize more effective and efficient global IT governance since CobiT's mission is to "research, develop, publicize and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals". (CobiT 4.1 March, 2010, Page 9)

Overall Success versus Partial Success

CobiT 4.1 defines IT governance as "the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives." (CobiT 4.1 March, 2010, Page 5) Therefore, IT governance should be consistent with the company's overall strategy and long-term goals. A new worldwide standard released by ISO in 2008 puts forward six principles for governance of IT: Responsibility, Strategy, Acquisition, Performance, Conformance, and Human Behavior. ISO/IEC 38500 also recommends that directors should govern IT through three main tasks: Evaluate the current and future use of IT; Direct preparation and implementation of plans and policies to ensure that use of IT meets business objectives; Monitor conformance to policies and performance against the plans (Hamidovic, 2010, Page 2).

While CobiT stresses the responsibility of corporate management, ISO points out the importance of evaluation of current and future use of IT in a long-term vision. ISO also brings up human behavior as a principle of IT governance which focuses on "IT policies, practices and decisions that demonstrate respect for human behavior, including the current and evolving needs of all the 'people in the process'." (Hamidovic, 2010, Page 2). All of these help corporations focus on the big picture in order to achieve long-term overall success. However, business leaders want the business to succeed and they will work hard to make that happen, but all too often, they are motivated and rewarded by having their small part of the organization succeed instead of having the big picture in mind. "IT governance requires that the scarce resource of technology capacity be diligently distributed across the organization for overall business success." In other words, it requires that IT cannot only be allocated on the basis of individual team needs but also - and mainly on collective, organizational goals (Reichental, 2011, Page 1).

CobiT framework helps us achieve this by being business-focused, process-oriented, controls-based and measurement-driven. "Managing and controlling information are at the heart of the CobiT framework and help ensure alignment to business requirements" (CobiT 4.1 March, 2010, Page 10).

Summary

As an integral part of corporate governance, IT governance ensures that IT goals are met and IT risks are mitigated by delivering value to sustain and grow the organization. CobiT helps with IT goal setting and achievement by identifying 34 processes in its four responsibility domains - Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME). For each of these 34 processes, a link is made to the business and IT goals that are supported. Information on how the goals can be measured, what the key activities and major deliverables are, and who is responsible for them is also provided (CobiT 4.1 March, 2010, Page 13). IT governance also drives strategic alignment between IT investment and program delivery and must judiciously measure performance.

To successfully achieve these goals, IT governance should be implemented with the consideration of national culture versus corporate culture and overall success versus partial success – both the macro aspect and the micro aspect. Though CobiT does mention in PO10 Manage Project that "Management of the process of Manage projects that satisfies the business requirement for IT of ensuring the delivery of project results within agreed-upon time frames, budget and quality is optimized when a proven, full life cycle project and program methodology is implemented, enforced and integrated into the culture of the entire organization" (CobiT 4.1 March, 2010, Page 72), it overlooks the influence of the national culture in which the corporation resides. Also, while emphasizing the overall control objective of a corporation's IT governance, CobiT doesn't put enough control over the potential negative effects from departmental nearsightedness. In order to implement IT governance efficiently and effectively, CobiT may consider developing further control guidance in the two areas above.

Sheila Swan Essay:

Reducing IT Security Breaches

"Sony keeps it honest after latest security breach." "Zappos latest company hit by data breach." "Philips Electronics suffers website security breach as hackers strike." These are just a few security breaches that made national headlines in the past six months. Information systems have become more challenging than ever due to the rapidly evolving technology environment. Many professionals are left seeking solutions for the current problems. Meanwhile new problems are arising. One potential idea to decrease security breaches would be to implement a government-mandated requirement, similar to that of Sarbanes-Oxley in relation to financial reporting and HIPPA in relation to personal healthcare information.

Since the issue of IT security breaches is increasing, alternative action needs to take place, however a government-mandated requirement is not the answer. Yes, the mandate would serve as another control holding companies and management accountable and responsible, but the cost benefit of such act is not reasonable. The cost of implementing such a mandate would outweigh the benefits for several reasons starting with the rapidly evolving technological environment. Another cost would be the broadness of the mandate. Finally, technology is somewhat proprietary in nature and uniformity and compliance would diminish uniqueness and competitive advantage for many companies, especially those serving specifically in the field of technology security.

The realm of technology is changing day to day. Technology is one of the fastest growing aspects in business. Jobs in the technology field exist today that did not exist twenty years ago, such as network engineers and IT developers. Ten years ago, "blogger" was not a position for hire. Today, jobs in cloud computing are replacing jobs created twenty or ten years ago, and cloud computing jobs just emerged within the last few years. Technology evolution is so rapid that a government-mandated requirement would cost billions to keep relevant and address all or even most of the IT emerging issues.

Unlike the earlier example of Sarbanes-Oxley as related to public financial reporting, the environment is changing too rapidly for a mandate. Public Accounting has evolved over the past twenty years, ten years, and even the past six months, but not nearly to that extent of technology. This shows Sarbanes-Oxley to be a cost effective government-mandated control. For an entire decade, the Sarbanes-Oxley Act of 2002 remains in effect, with several amendments to allot for accounting changes and evolution. The reason being, accounting is still basically the same. One decade from now, a government-mandated IT compliance act would be obsolete and null. In ten years, technology will have improved, evolved, changed, transformed and so on, more than we can imagine. Implementing a government-mandated requirement would drain federal dollars just to stay relevant from day to day. The cost of this control does not outweigh its benefits.

Cost benefit also leads into another problem with a government-mandated requirement for IT security controls. Which companies, industries, and organizations will the mandate effect? As mentioned above, Sarbanes Oxley relates to public companies. HIPPA relates to the healthcare industry. An IT government-mandated requirement would relate to whom? The requirement would have to cover a broad range of industries and companies. The cost to the federal government to cover such a range of industries and companies would be outrageous, let alone the cost to the industries and companies to implement the mandates.

The mandate would be put in place to protect specific stakeholders, such as the other mandates we have been discussing. Sarbanes-Oxley protects financial statement users such as investors and creditors. HIPPA protects private healthcare information such as diagnoses and treatment related issues for patients. Who would the IT mandate protect? IT breaches affect a broad array of stakeholders ranging from customers, employees, and even the company itself. The cost to incorporate this heavy of a mandate would not outweigh the benefits since the mandate would require so many provisions to accommodate for each type of stakeholder.

The industry range is also way too diverse. Not only are publicly traded companies affected by IT security breaches, but so are private companies. Large companies as well as small companies fall just as vulnerable to information security breaches. Governments and non-profits would also need the same regulations. Basically any company with a computer system, database, or even an email address would be required to follow the mandate to protect the effected stakeholders. Again, the government-mandated requirement for IT security would not be cost beneficial for several companies and would ultimately lead to failure in implementation.

One last case against the implementation of a government-mandated requirement argues that the mandate could do more harm than good. A multitude of organizations would argue that disclosure of their IT security would decrease the strength of their security strategy. Often security strategies are considered proprietary to the company, especially those companies specializing in IT security. Transparency of IT security controls would only provide an open door for intruders into the system being protected. Complying with a government-mandated standard would only impair the objectives IT security. Again, costs associated with a government-mandated act prove to outweigh the benefits.

Since a government-mandate does not seem to be the answer to protecting stakeholders from IT security breaches, what else makes sense? The Information Systems Audit and Control Association (ISACA) has offered a framework for best practices in information security called Control Objective for Information and Related Technology (COBIT). While this is not mandated for every company to incorporate into their information system, this is a great start. COBIT provides framework by aligning business goals with IT goals. Any company, large or small, in any industry, has access to this framework via ISACAs website. But the access alone does not decrease the risk of IT security breaches. COBIT is merely a tool for implementing effective internal IT controls. Again, it is not required and some companies will not implement COBIT framework. And just because some companies will implement it, the chance of an IT security breach will not be eliminated, but will be decreased. COBIT is only designed as a framework for this type of issue, not a solution.

I truly believe there is no solution. IT security breaches are inevitable. Even if a government-mandated requirement were to be placed in effect, IT breaches would still happen. Sarbanes-Oxley did not eliminate financial statement fraud and HIPPA violation law suits are filed on a daily basis. Unfortunately and simply, there is no solution. Effective internal controls, especially those lied out in the COBIT framework will decrease the chance of a breach, but will not eliminate the possibility of it.

Deliberation over the possible creation of a governmental-mandate should cease as this will have little effect in preventing security breaches. The cost to implement such mandate is enormous to both the companies and the government, mostly because of the rapidly evolving technology, but also because of the vast amount of companies, industries, organizations, and individuals it will effect. It’s also possible that the requirement objectives could open doors to intruders instead of close them.

Companies need to keep in mind that the risk of an IT security breaches are inevitable. Closely held, effective controls are the best deterrent. The COBIT framework can help any business implement effective internal IT controls. Ultimately, stakeholders “be aware”, IT security breaches are on the rise and will never be eliminated completely.

Junior Bernadin Essay:

Mobile Devices: The Network Security Nightmare

Mobile technologies are increasing in an alarming rate in our current society. The majority of professionals utilize mobile technology as part of their everyday lifestyles. Mobile applications are being developed daily to provide users with the ability to unlock the full potential of their devices by integrating and streamlining the user experience. Unfortunately, these advantages come at a great cost, security. "These mobile devices all have access to your corporate network via email, VPNs, and other remote access methods." (www.mcafee.com) Access to these enterprise systems by these type of mobile devices are an added network risk as their connections can serve as inflection points.

These devices are being used to access and mange unusually high amounts of data. As information management on these devices became an issue for many users, developers created applications that allow these mobile devices to synchronize data to a desktop or cloud solution. Using this feature although convenient, exposes sensitive organizational data to systems that are not manageable by the companies IT department. Since most of these devices do not have intrinsic security features built in, most rely standard password authentication. "Security attacks are also on the rise, with 43% of respondents indicating there has been a significant increase in the frequency of cyber attacks over the last year, and 77% saying these attacks have become more severe or difficult to detect/contain." Gabryluk (2011). Hackers even utilize malicious Wi-Fi spots as an attractive means to obtain data from these types of devices.

With such vulnerabilities amidst, mobile apps are still being produced in an alarming rate in response to user and competitive demands. "The increase in mobile device deployments has also brought an upsurge in mobile security threats. A study by Juniper Networks revealed that last year brought a 250% jump in the number of threats in the mobile space from malware and viruses". Konstant (2011). This push however has focused on the development of the application not the security vulnerabilities that are on the rise. Thousands of Facebook, Twitter, and other popular mobile applications have been hacked over the past couple of. As these types of apps access information located on the mobile device, this information is obtained when a device is hacked. This presents additional problems for IT personnel as they are charged with the task of securing these devices. "The Ponemon Institute, in research sponsored by Juniper Networks, has found that 90% of businesses report having fallen victim to a cyber security breach at least once in the past 12 months." Gabryluk (2011). Mobile devices also tend to use Bluetooth technology which opens the device more vulnerabilities as well.

Hackers have been exposing these vulnerabilities on various scales. In June 2005, the Lasco mobile malware worm was found to replicate itself to other Bluetooth devices and render the device unstable. As Bluetooth security tightened after the vulnerability was exposed, hackers have turned to Bluetooth Pin and Linkkeys Crackers as a means bypassing device security. In May of 2011, Sean Keveleighan, head of Communications & Public Affairs for Citi, announced that "During routine monitoring, we recently discovered unauthorized access to Citi's Account Online. A limited number – roughly 1% – of Citi North America bankcard customers' account information [such as name, account number and contact information including e-mail address] was viewed" Rogers (2011). Nintendo announced in June that it was also the victim of an intrusion although no personal data or corporate information was lost. Sony on the other hand was not as fortunate.

The hacking of Sony's systems revealed that data was lost for over 100 million users through a vulnerability found on the network service for Playstation 3's network. This information was considered a massive data loss that included information such as: Name, Date of Birth, Email Address, Account Information, User ID, and Possible Credit Card Information. Ironically, this is the same network that is utilized by the Sony PSP, the mobile Sony Playstation device.

Many security corporations have begun taking a stance against rising mobile threats and implemented a system to secure their networks. McAfee for instance provides a Mobile Security Assessment service that serves to expose and define the vulnerabilities in your corporate network and infrastructure. This assessment also analyzes the backend servers that mobile devices within the company utilize. This assists IT departments with understanding the risks associated with using specific mobile applications as well as best practices to be used to support them. Other companies like SonicWall are including mobile security as a part of their overall security plans. "With the risk of confidential data leakage ever increasing and the old generation of firewalls is ill-equipped to handle these new threats, SonicWall presented its next-generation firewalls that offer real time traffic, highest performance networks delivering full application intelligence, control, and real time visualization and inspection to stop threats and prevent data leakage with no latency. " Ajou (2011).

SonicWall is not alone as more companies are joining this security battle and using their specializations create a piece of mind solution for their customers. In June 2011, Zenprise launched the ZenCloud, a cloud-based mobile enterprise security and device management system. This cloud utilizes 100% SLA and approaches the mobile vulnerabilities by managing them through a central, secure, and closed-looped environment. "To protect the entire mobile enterprise, Zenprise has built solutions from the ground up to offer products that are scalable, fault tolerant and resilient," said Jayaram Bhat, Zenprise CEO. "Since any outage can potentially create security vulnerability, today's announcement of our new cloud based solution and 100 percent SLA demonstrates our uncompromising level of service and support while backing it up financially" (www.sourcewire.com). Zenprises' solution focuses on the access points and management of the devices instead of attempting to manage those devices on the network level.

Another safety net that is being utilized by companies is a total device wipe. As this may not help much from an application breach standpoint, it is definitely useful for scenarios where mobile devices that are lost or stolen. As these devices tend to store confidential information it is imperative that the data is discarded appropriately if the device is lost. "There are a whole lot of technologies being used but not overwhelmingly, the main one is remote device wiping, while securing access to corporate data is done at the application level." Raywood (2010). Companies like GadgetTrak and Lookout Mobile security specialize in these data wiping and protective services. There have also been other cases where this type of technology was used to recover the lost/stolen device. At the end of May 2011, an article went viral about the theft of Sean Power's computer. Using a software application called Prey, Sean was able to locate his device, capture valuable data about the thief as well as protect confidential resources on his computer. As mobile devices are powered by applications, some companies such as apple have a system in place for screening their applications as part of their threat-prevention procedures. This assists in providing a safe environment for mobile devices and corporations as a whole. It is evident that companies are now taking note and implementing new strategies to secure their products and environments.

Analysis

Research on mobile devices and network security indicate that there are various methods that can be used to create a safe and secure environment for mobile technology. As there is no one solution to security, solutions need to be administered in conjunction with key methods. One area of concern is securing the devices themselves instead of making exceptions for mobile devices. On the corporate level, these devices should be treated just as any other piece of network equipment would be treated. To do this, appropriate security software should be installed on these devices. Software that protect against viruses, Trojans, SMS or email phishing, rogue applications, and other malware are be ideal for corporate network protection. Network access control capabilities are an additional feature that should be considered when selecting software. Please note that any software used on these devices should only be downloaded from a stable and trustworthy publisher and/or environment.

Ensuring that the correct management tools are installed on mobile devices and their compatibility to manage and configure devices on the enterprise level is a must. This type of management helps ensure that the network remains secure and limits the vulnerabilities on the device itself. Another useful security solution would be a system that addresses the lost of devices that contain confidential company information as well as data leaks. To address these concerns, many have required strong password authentication in conjunction with remote lock and wipe capabilities. This provides an additional solution to data protection, even in cases where the device is not retrievable.

In addition to solutions mentioned above, changes on the network level are also required as network security is expected to keep up with rising threats that present themselves. Application-level security must be implemented on the network to ensure that the network secures itself from outside attacks. A recognition tool is also needed so that the network can identify any potential threats introduced to the environment by a mobile device.. All of these solutions do require constant research and insight on the latest threats and improved security practices to ensure the network meets today's standard.

Furthermore, a key solution to mobile security in any corporate environment is the implementation of policies to ensure that the organization as a whole is utilizing best practices. Data leakage policies are a must as employees must know how to treat sensitive corporate data as well as effectively communicating its importance. Policies that help with understanding risk data loss are an added measure that could be used to improve security. Network-wide policy controls and enforcements are other key tools that ultimately help secure a network environment. These policies should include strict user permissions on data as well as data encryption for data when in traffic or at-rest.

Conclusion

There is obviously a gap between the development of mobile apps and the security of these apps so it is imperative that the correct processes are in place to prevent viruses, mobile hacking, and identity theft issues on both personal and corporate levels. With mobile threats in their infancy, now is the time to place mobile security at the forefront of network security. Mobile devices should no longer be allowed to operate on a corporate network as an exception to the rule. Mobile devices should be secured through software, compatible enterprise management tools, data-loss protection software, and the education and implementation of security policies. Together, with the help of stricter policies on the mobile application environments, corporations will be able to have a solid network security system with a stable mobile environment.

Yulin Wang Essay:

Problems in Implementing IT Governance and Solutions from COBIT4.1

Introduction: Information technology plays a more and more important role in today's business world. Compared to the previous decades, when it was mostly used in back-office areas such as data storage and workplace communication, now IT governance functions as a more powerful tool to support enterprises in achieving long-term business goals. But what is IT governance? In COBIT 4.1, the definition is that "IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives." (ITGI, 2007, p. 5) Even though most directors have realized that they need IT governance and also have taken the initiative to implement IT projects within their organizations, they have encountered significant problems and difficulties. According to 2011 Global Status Report on GEIT, 21% of enterprises noted their projects were ended before full implementation because of their shrinking budgets and the poor performance (ITGI, 2011, p. 20). I would like to demonstrate some common problems and difficulties in IT Governance.

First, on the company level, it is difficult to reconcile the IT strategy with business strategy in an economic downturn. The 2011 Global Status Report on GEIT highlighted that nearly 40% enterprises are suffering from increasing IT costs (ITGI, 2011, p. 18). As a result, the

CIOs have difficulties in convincing other board members to sacrifice the short-term economic benefits so as to implement a long-term IT project that may have no promise of success. In addition, CIOs are also facing problems when they do the cost-benefit analysis of different IT projects, that is, how to decide the priority of IT projects under a limited IT resource situation. CIOs have to coordinate with other department leaders to determine the most appropriate projects to deploy, and there are obvious trade-offs in this process. CIOs admit that it is impossible to satisfy all IT support needs and communication problems frequently emerge when deploying IT projects. Accordingly, 41.2% of enterprises listed communication issues as the challenges and this problem was the one with largest percentage (ITGI, 2011, p. 33). Regular staff with a weak IT background can hardly understand the ideas from IT staff. Their resistance to new technology always exists because of the longstanding habits. All in all, the problems could be considered as the lack of alignment and compliance in implementing IT governance within the organization.

Second, the availability of IT experts is limited. In 2011 Global Status Report on GEIT, 34.4% respondents indicated that they have insufficient IT staff and 31.3% said their IT workforce have insufficient IT skills (ITGI, 2011, p. 18). Outsourcing IT governance requirements is a good way to cut expenses and solve the human resource problem, but it will introduce the security problems into enterprises at the same time. Furthermore, the problems also lie in how IT experts including the CIOs understand their positions. Are CIOs also business leaders? Are CIOs still staying outside the mainstream management of their enterprises? Should IT staff know more about business operations in order to fix the targeted problems in the system? Absolutely, what most enterprises really need are experts who could perform in both IT and business areas. However, IT experts with business background are not always already available in job markets and thus need training, which also increase the cost of IT governance. As I mentioned, CIOs work as coordinators in different departments, and they should recognize that their mission is to achieve the long-term business goal of the enterprises. Again, not every company would be able to find the exact person who could understand all the business operations and lead the IT changes in the whole enterprises.

Last, the risk management of IT governance should not be ignored since 93% respondent in Global Statue report fully or partially outsourced some of their IT activities (ITGI, 2011, p. 35). If enterprises seek outside IT services such as public cloud computing, they are inevitably involved with high risk since the business data, including trade secrets, may be exposed to a third-party or, more seriously, to their competitors. Because of security and data privacy concern, 57.5% enterprises will not use cloud computing for mission-critical IT services (ITGI, 2011, p. 37). New technology proponents possibly argued that there is nothing wrong with new technology itself, but what we could not deny is that risks come up when we adopt it in our enterprises' IT structures. CIOs try to deal with the "irrational fears" about cloud computing and also to reinforce the security level of their company's IT system. To be honest, this process is slow and tough because it depends on how CIOs define the irrational fears and the specific IT structure of their companies.

Fortunately, we could figure out solutions to these problems using COBIT4.1, which is a manageable and logical framework designed to guide IT governance implementation in enterprises. In 2009-2011, COBIT 4.1 has already used by 12% of respondent enterprises (ITGI, 2011, p. 29).

To bring down the wall between IT strategy and corporate strategy, enterprises should refer to PO4 in COBIT4.1, "Define the IT Processes, Organization and Relationships". According to the maturity model in PO4, the problems mentioned above indicate that enterprises are at a repeatable but intuitive level (ITGI, 2007, p. 46), which means IT organization and relationship are established but are not agile enough to respond to the needs of stakeholders. First of all, CIOs should define an IT process framework that takes all possible stakeholders into consideration including C-level executives, IT staffs and end users. The second step is to build an IT steering committee under the established IT framework in the first step, and this committee is responsible for deciding prioritization of IT programs and allocating IT resource among various programs. The rationale within these steps is to bridge the gap between IT and business governance by providing communication and collaboration chances to different stakeholders. With the committee, IT staff could better respond to the business needs, and regular staff could better understand the IT procedures in a common language, which will eventually lead to the improvement of IT project performance. Actually, 33.3% of enterprises have already planned or implemented some kind of collaborative program to make IT staff and business work together (ITGI, 2011, p. 41), but a steering committee mentioned in COBIT is more centralized and effective.

PO7 provides framework to manage IT human resources. Enterprises rely on competent IT workforce to deliver IT services, but many of them do not have a well-established system to maintain this scarce resource. The most serious problem is that the training funds could not be ensured due to the economic downturn. As discussed above, CIOs could work with the IT steering committee to make financial budget for training programs in advance and guarantee that training funds will not be sacrificed to meet other financial requirements. Both the board and CIOs need to keep in mind the importance of IT human resources and the necessity of training programs which will enable their IT staff to update skill sets. In addition, more emphasizes should be put on IT agility so as to reduce the resistance from end users and to increase the compliance of IT implementation. So CIOs should help IT experts understand their roles in IT governance of enterprises as well as encourage IT innovation such as new delivery methods and security tools.

As Dr. Jonathan Reichental said in his article, the CIO should not think of himself as the chief information officer but rather as the chief inspiration officer of the organization (Reichental, 2010).

To manage IT risks, CIOs could apply the tactics stated in PO9 to their own enterprises. CIOs should integrate IT risk management with the enterprise's risk management framework under the help of CEO and CFO. Different companies have different risk appetites and risk tolerance levels, but IT risks have to fit in the enterprise's risk appetite. Then risk context should be identified by business manager so that CIO could link events that might influence the final objectives of enterprises to the potential risk issues. After the risks have been identified, the CIO and other business executives begin to evaluate the risk and prepare appropriate responses to it. One might notice that not only the CIO but many business executives are involved in IT risk management and this might slows down the risk management process. But a professional risk management framework could effectively eliminate the irrational fears because people know the company is under robust protection. With respect to the cloud computing and outsourced IT service, C level executives have to make a thorough investigation on the demand of outsourcing, to determine the related risk tolerance ability and then to monitor the performance of the service. Finally, all the frameworks and system should follow up with the changes in business strategy, financial situation and business environment.

There are abundant examples of successfully applying COBIT4.1 to enterprises' IT practices in different industries. Maitland, an international firm providing health services, utilized COBIT4.1 to improve the communication mechanism between business and IT departments and increased the IT governance maturity level by achieving a shared understanding and vision (Brown, 2011). Another example is that Grupo Bancolombia, a financial institution operating in multiple countries, utilized COBIT4.1 successfully as well. Even though it has already established internal IT control policies, the compelling alignment needs resulted from the wide-range operations in different countries forced the board of directors to choose a more complete IT governance framework. COBIT4.1 worked well after being adopted and improved the business operation performance (ITGI, 2011).

Summary: COBIT4.1 is a useful guide to solve problems in implementing IT governance. The key issue in making your IT system work smoothly is to enable different executives to communicate efficiently and to enhance the understanding between IT staff and end-users. In one word, the ability of an enterprise to reconcile conflicts in IT governance and corporate governance decides its success in utilizing IT governance to achieve business objectives.

Kyle Torres Essay:

IT Security and Mobile Technology

In a constantly changing world of technology, the need to understand and strengthen IT security has become more and more important. The use of mobile technology in the form of tablets and phones has created a new area for consideration when it comes to IT security. Although the future of this technology is unknown, it appears that mobile devices, and the market around them, will continue to develop. Everyone must consider the potential risks associated with mobile technology in order to remain safe both physically and online.

What is Mobile Technology?

Mobile technology includes, but is not limited to, cellular phones, tablet devices, mp3 players, and laptop computers. The demand for such devices has continued to increase over the last decade as prices have continued to drop, making the technology much more accessible. Individuals have maintained an "always on" status in terms of their ability to stay connected to the internet at all times. Users of these devices take advantage of the capabilities of each extensively. Since the creation of mobile applications, people have started to interact with their mobile technology much more than ever before.

Why does it Matter?

The continued use of mobile technology appears to be a value added component to everyday life. Although one can debate the credibility of this statement, it is important to note the pros and cons associated with this dependency on technology. People are able to connect to email, weather, chat, and the internet at virtually any point throughout a given day. This connectivity can help to increase efficiency as a business, or promote a new marketing technique to increase sales for a particular business. The use of mobile applications can assist a user with their banking needs, schedule coordination, and even entertainment. What people do not often realize, however, is how the providers of such applications actually retrieve data about the user. Even a simple game on a phone can send information about a user's activities to companies who then profit off of this data. A mobile device, though a tool to assist individuals, can actually be used as a weapon against them.

Ways of Obtaining Information

When it comes to retrieving information from a mobile device, companies and application providers have many tools at their disposal. Many of the techniques used to gain user information are performed without user knowledge, or without clear indication of the behavior. Whether a person uses a phone to connect to their email, a tablet to play a game, or a computer to type a paper, companies all around the world are retrieving data about people to use to the company's benefit. One of the first bits of information companies can retrieve is called metadata. People often take pictures using mobile devices, but they do not always understand that a picture contains much more data than simply the image produced. Metadata is information stored within the picture, including the time and date the picture was taken, the type of camera used, resolution, Torres, 2 and more importantly, location information in the form of GPS coordinates. Most mobile devices come equipped with GPS, allowing the user to track their own location at a given time. The camera application on the mobile device often opens with "Store Location" turned on by default, storing location data. This metadata can then be downloaded by a company or individual with free, easy to use software readily available online. Though this location information may seem harmless, the endless possibilities of what others can do with the data should be reason for concern.

A recent study from the Leeds School of Business at the University of Colorado Boulder found that 23% of the 90 websites examined do not remove this location information from photos uploaded to their site. This creates reason for concern as individuals using the website are unaware of this error, but they are at risk of being targeted by predators. Many profile pictures on these dating websites are taken with cameras and mobile devices capable of storing location information. If a user takes a picture at his or her house, or place of work, someone else can use this against the individual. Without proper communication and awareness of this location information, users are placed in real danger without knowing it.

Along with this location information come the fear of user habit tracking. Many reports in the news indicate various companies storing location information about a user at any given point in time. This knowledge makes mobile technology users vulnerable to corporate eavesdropping. Mobile devices are often used in conjunction with a cloud-based service such as Apple's iCloud, Google, or even a mobile network provider like Verizon. These services attach the user of the mobile device to a database stored with personal information. With this information, companies can take advantage of the user's lack of knowledge to make various decisions based on habits generated by their location. This information becomes very valuable to the organization, and potential hackers, who look to gain from user behavior. Despite a company's greatest efforts to maintain a secure IT infrastructure, people somehow find a way into the database, exposing the personal information of millions of people.

One of the most common uses of mobile technology comes in the form of applications. Users interact with applications throughout the day, and often without knowing their personal information may be pulled from their phone and sent to a third-party. Upon installing an application, the user is presented with a list of security access permissions, many of which contain jargon the user cannot understand. The user will click "Accept" which agrees to allow the application to obtain information from a phone. A user may unknowingly accept certain terms, and ultimately agree to allowing the app to listen in on phone conversations, read and write to the memory card, track key presses, and read contact lists. This information is immediately sent to servers at a third-party, which is then sold to companies. The value of an individual's personal information is literally translated into a dollar amount for companies.

What this Means for People

As the demand for mobile devices continues to increase, opportunities for privacy invasion as the result of third-party intervention will increase as well. At this point in time, only through individual awareness and action can these infringements be prevented. Situations such as the accusations against Facebook, the research done at the Leeds School of Business, and exposure of mobile network provider wrongdoings will only help to educate people on the importance of making informed decisions on a mobile device. This awareness can assist with protecting individuals in the real world by stopping threats before they happen, and preventing businesses from capitalizing on personal information without user knowledge.

President	Matt Randolph (720) 931-4594
Executive Vice President	Ram Ramadoss (720) 578-3336
Past President	Brennan P. Baybeck
Secretary	Tim McCain
Treasurer	Don Mapes (303) 600-2892
Membership Vice President	Scott Peyton
Education Vice President	Rick Lucy
Education Committee	TBD
Academic Relations Coordinator	Rhonda Willert
CISM Coordinator	David Vos
CISA Coordinator	Mark Gengozian (303) 807-2877
CGEIT Coordinator and Research Liaison	Koushik Kumaraswamy (303) 810-6719
Communications	Casey Lems
Social and Networking Committee Chair	Mary Bloomingdale
Sponsorship Chair	TBD

About Us

The Denver Chapter of ISACA® (formerly EDPAA) was founded in June 1976 with just a handful of members. Today, the Denver chapter with over 800 members, is one of the largest chapters within the Southwestern Region. The Denver Chapter contributes to the international organization with financial support and periodic hosting of the International Conference.

Mission

The Denver Chapter of ISACA® is a non-profit organization dedicated to the continued development and enhancement of the information systems audit and control profession by providing benefits to its members and to the professional community-at-large.

ISACA®

Trust in, and value from, information systems

Denver Chapter