

November 2011



Newsletter

Our Mission: Provide our members opportunities for career development and networking with peers. Advance and promote the profession by creating awareness of the skills and abilities of IT audit and security Professionals.

Greetings Utah Chapter members,

We will not be holding a November ISACA luncheon as we just finished our Fall Seminar last week. It was a great event and thank all who was able to attend.

We can get a head start on advertising for our December luncheon as we will have Dr. Conan Albretcht from Brigham Young University at our monthly luncheon on December 16, 2011 speaking on the topic "Picalo, an introduction to an Open-source Data Analysis Library and Platform." Here is a brief intro about Conan and his topic.

Picalo is a data analysis application, with focus in fraud detection and data retrieved from corporate databases. Professor Connan Albrecht created it as the foundation for an automated fraud detection system that is free and open source. He has used in financial services environments world-wide.

Picalo is currently focused on data analysis for fraud and corruption detection. However, it is an open framework that could actually be used for many different types of data analysis: network logs, scientific data, any type of database-oriented data, and data mining.

Connan Albrecht is an Associate Professor of Information Systems at Brigham Young University. He teaches intermediate and enterprise Java programming to students in the ISys Core. His research topics include computer-aided fraud detection, group support systems, and ecommerce architectures.

When Professor Albrecht is not teaching, researching, or developing, he spends time with family, mountain biking, reading, fishing, hunting, snowmobiling, and skiing.

You can register for this event on the ISACA website (<http://www.isaca-ut.org/utahevents.html>).

Thanks

Josh Taylor

Newsletter Editor

Monthly Professional Training

Date: Thursday, December 15, 2011

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Conan Albrecht

Topic: "Picalo, an introduction to an Open-source Data Analysis Library and Platform"

Cost: \$20 for members and \$15 for students, \$25 for non-members

CPE: 1 Credit

Register at: <http://www.isaca-ut.org/utahevents.html>

Monthly Training Registration

The cutoff time period to sign up for the professional lunch meeting is the Tuesday before the monthly Thursday meeting. If you sign up after noon on Tuesday, you may or may not have a guaranteed seat. Since the rooms at the Lion House are small we have to give them a hard count by Tuesday at noon to reserve a room.

Earning CPE

ISACA e-Symposium

If you are in need of CPE credits, an easy way to earn them is by participating in an ISACA e-Symposium. These are free online web casts and you can earn 3 CPE credits. For further details, go to: www.isaca.org/webcasts

There is no limit to the number of e-Symposiums or on-line quizzes that you can take to help fulfill your CPE requirements. If you have any questions concerning CPE credits please email the following: certification@isaca.org and they will answer your questions.

Monthly Article

Culture of Security

Surely this is just another dissertation about how creating a culture of security in your organization is going to reduce childhood obesity, increase your ROI, and bring world peace. No reading this piece probably won't accomplish all those things but it will lighten the load on most organizations in their efforts to stop insider security threats.

In their efforts to create a culture of security, managers lean heavily on auditors to help in their efforts, but too often auditors hear these refrains:

- I know I am not supposed to have access to this information, but I was granted authorization in my old position and I just kept it when I was transferred here.
- Management authorized these monitoring tools, but they didn't give me any budget for people to do the monitoring.
- Yep, I sure do support IT security, but if there is going to be a company to secure, departments like mine need to show they are making money first.

Put in succinct terms an organization's culture is defined as what an enterprise actually does about security and not what it intends to do about it. This means that a culture of security doesn't belong to the security department, the legal department or the chief executive officer. The culture is generally felt and exercised across the expanse of the business from the corner offices to the basement. It is the spirit of the times, the "zeitgeist" of the business's composition.

The status of security is the level of its desirability, but not at any price. Of course not. The truth is security implies a certain level of acceptable risks which raises the question who then determines set of decisions relating to those decisions. There isn't any set of policies or standards that might hope to quantify all possible circumstances that can be predicted.

Prevention of malware and malicious attacks are merely a part of the security picture. By extension security encompasses stored information and data that are currently part of business production activities. Of course within the confines of this structure is the value of information including all its inherent risks and costs. It is the value of data that is the limiting factor deciding its appropriate level of security. In short one doesn't build a \$5,000 fence to protect a \$200 horse. And it is the culture within a business organization that instantly recognizes this fallacy.

Sound security is perceived by most enterprises as a prerequisite for doing business with other organizations. They must ensure the confidentiality, availability and integrity of information and the same level of operational systems managing that information. For without these basic ingredients customers will simply look to competitors to do business. And the same holds true with the organization's business partners. Without the extensions of CIA among organizational partners, the culture of security cannot exist to an extent that successful operations cannot exist. If the customers were to learn the site or the processes were not trusted the business would certainly lose sales and customer confidence. Consequently, online and brick and mortar businesses have painfully learned that customer confidence is strategic and data security is an integral component of that strategy.

Many executives are fond of asking the seemingly tough question of "what does this cultural shift of security do for our bottom line?" So exactly what is the effect on ROI? Well the answer is pretty simple. It might be viewed as a competitive advantage when the business has a high degree of trust of its IT systems and those belonging to its partners. A practical example of this business model is Amazon.com. They drive customer satisfaction knowing their personal and credit information is safe from malicious attacks as part of their branding. It is worth noting these organizations are for the most part loath to broadcast their security measures as they do not wish to overly publicize their protection infrastructure.

Yes fraud prevention is still an element of security where the environment possesses data of intrinsic value. It is widely recognized then that the importance of security lies in the preservation of information as an asset. Nevertheless for many people, the value of security is to merely preclude “bad” things from happening. At least in this lens then security is essentially reactive.

However significant fraud and misuse of data are indicators of failures of security. But on the flipside of the coin, it is impossible to establish a positive picture of security that is without failures. A culture of security must be founded on the contributions that security makes to an organization’s strategic objectives. It is the integrity of the organization’s employees that contributes to a culture of security. In other words, if only the interaction of the community’s people have with the police when a crime occurs, they will not have any appreciate of the rule of law for an ordered society.

Consequently, if the only intervention employees have with security within their organization happens when a policy is violated, they will not have any appreciation for a culture of security and they will view security as an impediment to their function.

Alan B. Sternecker, CISA, CISM, CFE, CISSP is a consultant and author of Critical Incident Management, ISBN: 084930010X, published by CRC Press, www.crcpress.com. He has written numerous articles and regularly lectures regarding fraud and computer systems security auditing. He can be reached at absterneckert@yahoo.com

Board of Directors and Officers

Can be found on <http://www.isaca-ut.org/administration.html>

The views and opinions contained in this publication are solely those of the authors, and do not necessarily represent or reflect the view or opinions of the Utah Chapter. In the event you have any questions concerning an article, you may wish to contact the author directly.