



Information Technology Security Council December 2009

Information Technology Security Council Members

Chair:
Mr. Ronald Lander, CPP

Vice Chair:
Mr. Thomas R McElroy,

Mr. Shayne P Bates

Mr. Raymond J Bernard

Mr. Kevin V Bluml

Mr. George E Caldwell

Mr. Brent Campbell

Mr. James Keith
Flannigan

Mr. Robert L Foss

Ms. Caroline R Hamilton

Ms. Robin S Harris-
Walker

Mr. Matthew D
Hollandsworth

Mr. Thomas J Ianuzzi

Mr. Henry M Kluepfel

Mr. Kelly J Kuchta

Mr. Ronald L Martin

Mr. Werner Preining

Mr. Lewis E Wagner III

Mr. Reginald J Williams

Mr. Richard A Withers Jr

Mr. Coleman L Wolf

Mr. Steven T
Yanagimachi

From the Chairman:

This is the inaugural edition of the ASIS Information Technology Security Council's outreach communication with the ASIS membership. The Information Technology Security Council and its partners deliver forums, such as this newsletter, to enhance effectiveness and productivity of security practitioners with educational programs and materials that address specific security concerns related to Information Technology. Every quarter, we will provide this newsletter to distribute high-impact briefings regarding contemporary subjects of interest to the membership. These articles are available for reprinting as long as the author and source is attributed.

If there is a subject for a future newsletter that interests you, your chapter or council, feel free to send me an email at rlander@ultra-safe.com or call me at 800-334-6670. Also, the ITSC is active in chapter outreach and education throughout the year. If your chapter wishes to have a presentation specific to Information Technology, feel free to contact me, and we will identify a member near you.

Who's Minding the Store?

What Every Security Manager Needs to Know about Information Security
By Tom Ianuzzi, CPP, CISSP, CFE, CCE, President,
Information Security Consultants, Inc.

If you are the security manager in a small or medium sized organization, chances are that Your Company does not have a full time Information Security function. Instead, that job has probably been entrusted to the IT manager. If that's the case, there may be a few critical items that are falling through the cracks.

IT managers generally focus on the technical aspects of computer security. They seldom consider the broader view of information security. There is a critical difference. Most information loss is not the result of hacking or password compromise but rather is caused by employees misusing data that they have legitimate access to. By working closely with IT you can bring your security knowledge and experience to bear on the problem. Remember, the IT manager is usually a technical expert but often has little or no security training. In addition, he or she is usually facing huge demands for productivity and has little time to devote to security. As a result, important issues may be ignored.

Here are four that frequently lead to losses:

1. A lot of effort is expended protecting electronic records but, in many organizations, once they are printed all bets are off. Review your Information Sensitivity Policy to see if they

- accord equal protections to paper records. In not, they need improvement.
2. A lot of sensitive Information leaves companies on USB devices, memory sticks, portable drives, or PDAs. There are a variety of ways to disable the use of these devices. Find out if your company is using effective ones.
 3. Critical data on portable computers is often overlooked. This threat often goes undetected because no one realizes that the data is present. This happens when sensitive data is loaded to meet a short term need such as getting a marketing analysis done over the weekend. Although this information remains on the computer, the machine is still perceived as containing only public sales information. The only workable defense is to treat all portable computers as if they contain your most sensitive data all the time. Full drive encryption is a must. The IT department will know how to do it but, you might need to convince them that it is necessary.
 4. Social Engineering techniques can defeat even the strongest passwords. Unless you have an effective ongoing security training program, your co-workers will fall for these cons almost every time they are tried. Employee training is usually one of the weakest links in the security chain. You can do a lot to insure that your company has a strong effective program.

Although you may not have the technical background needed to protect the company's servers from the wiles of a cagey hacker, you do have security knowledge that is of immense value to the Information security effort. In addition, you are experienced in working with people to mitigate risk. If you bring your skills to bear and work closely with the IT manager, you can have a profound effect on your company's Information security program.

Cloud Computing – What is it and Why is it Important to You?

By Shayne P. Bates, CPP, CISM, CHSV, DABCHS
Executive Vice President at Brivo Systems

The term "Cloud Computing" is the subject of much discussion. What is the "Cloud", and how is it relevant to the security industry? What are the implications for business, technology, our industry and the end user customer?

Cloud computing is a term synonymous with Software-as-a-Service (SAAS), hosting, application service provider (ASP) and several other comparable terms. Think of it as an application moving from the desktop or server, to an online "Cloud" environment existing in one, or several data centers. Using the Internet to provide the connection, the application "in the cloud" is accessed using a web browser from almost any device such as your cell phone, laptop or desktop.

Is it new? The trend to move applications to the cloud has been underway for several years and is not a new concept. Timesharing on a mainframe computer for many customers is a similar model, but what has changed is the business model, maturing technology and capabilities.

Cloud computing is a byproduct of "Convergence" – a fusion (dictionary). The merging of different elements into a union) of technologies, process and people from the more traditional security and IT industries. Chances are that you are already using "the cloud". Examples include Web-mail or retrieving voicemail messages through your web browser. Salesforce.com is a cloud application delivered as an online service for customer relationship management. Salesforce.com has built a business that today, has over a million users who manage their customer opportunities "in the cloud".

Here's a powerful reason – the economics for the delivery of security services to those who could not previously justify it have changed – imagine controlling a small number of doors and cameras across a large number of geographically separate sites with no servers (for example retail and property management). All with no software application to support, and almost no IT overhead at the users site. For many, it's still an unheard of offering from many security manufacturers.

Security professionals who are able to articulate the business benefits of cloud computing to fulfill security requirements by the delivery of services are succeeding in developing continuing relationships with their customers. They are installing cloud-capable security devices on networks for their stakeholders and educating about the business issues and cost benefits of "pay as you go" arrangements.

A note of caution — relocating "old generation" servers to a data center and relieving the

management pain for the customer is not cloud computing. Although there are many differentiators, two significant ones to look for, that separate “true cloud” from the “stack-crowd”, are the existence of an online multitenant application, and whether that file server (with its costs) will really vanish. Savvy providers, who have invested in, and have experience with cloud infrastructure, know how to manage it so that user data does not disappear, and is available when you want it. Also - look for the existence of an independent and regular audit to a standard.

The ASIS Information Technology Security Council is presently developing a whitepaper titled “Cloud Computing and Software as a Service (SaaS) – An overview for Security Professionals”.

It will be published during 2010. This Whitepaper explains the compelling business reasons, technology, functions, legal and security issues that make cloud computing a paradigm shift not to be ignored. Sites with no servers (for example retail and property management). All with no software application to support, and almost no IT overhead at the users site. For many, it’s still an unheard of offering from many security manufacturers.

**Join the ASIS Information Technology Security Council (ITSC)
Today! Send your CV to: ITSC Membership; attn: Coleman Wolf
cwolf@edesign.com**



1625 Prince Street
Alexandria, VA 22314-2818
USA
703-518-1447
Fax: 703-518-1517
Email: councils@asisonline.org