HOW TO
Build Trust
When It
Comes to
the Cloud

Jim Goldman of
CloudOne and
J.J. Thompson of
Rook Security
outline strategies
to set appropriate
board expectations

Tackling Cloud
Data Sprawl

The ‘Softer’
Side of Security

5 Minutes with
Meng Chow Kang
The New Security

It’s as much about enabling business and customer confidence as it is about protection – CA software helps do both with secure application access, improved customer engagement and proven end-to-end security.

To learn more about how CA Technologies can help protect and enable your business, visit www.ca.com/openenterprise

Attending RSA Conference 2015?
Stop by our booth #3413 in North Exhibit Hall D

Keynote Information
Security - Rewritten By the Application Economy
Thursday, April 23rd at 3:50 pm
Amit Chatterjee
Executive Vice President, Enterprise Solutions and Technology Group
CA Technologies

Copyright ©2015 CA. All rights reserved.
(ISC)² Security Congress conferences make a global impact by securing tomorrow today at each event through the multi-track educational sessions along with prime networking and career advancement opportunities. Each Security Congress will include topics on best practices, current and emerging issues, and solutions to challenges.

(ISC)² Security Congress
Proudly collocated for the fifth year in a row with ASIS International 61st Annual Seminar and Exhibits (ASIS 2015)

28 September – 1 October 2015
Anaheim Convention Center
Anaheim, CA
congress.isc2.org

(ISC)² Security Congress EMEA
Organized in partnership with MIS Training Institute

20-21 October 2015
Sofitel Munich Bayerpost
Munich, Germany
emeacongress.isc2.org

(ISC)² Security Congress APAC

28-29 July 2015
Sofitel Philippine Plaza Manila
Manila, Philippines
apaccongress.isc2.org

Organized in partnership with

(ISC)² Security Congress Latin America

24-25 November 2015
Sao Paulo, Brazil
FEATURES

➤ MANAGEMENT
16 Building Trust with Boards
Two experts on strategic management explain how best to communicate technologies—particularly cloud solutions—to win over executives. BY JIM GOLDMAN AND J.J. THOMPSON

➤ TECHNOLOGY
22 What to Do About Cloud Data Sprawl
An (ISC)² member provides insights and instruction on how to rein in cloud-based data strewn all over the place. BY AARON SANDERS

➤ PROFESSIONAL DEVELOPMENT
26 Yes, It Is Your Business
An (ISC)² member makes a case for investing time and effort into the ‘softer’ side of professionalism. BY TONY VARGAS

Like a teenager’s room, you may want to shut the door and ignore the mess. When it comes to the cloud, though, you can’t. PAGE 22

InfoSecurity Professional is published by Twirling Tiger Press Incorporated, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)² on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To request advertising information, please email tgaron@isc2.org. ©2015 (ISC)² Incorporated. All rights reserved.
Editor’s Note

GOT TO KEEP MOVING

As a child, I was jealous of classmates who had lived their entire lives in the same hometown. It seemed they had stronger connections to each other and their surroundings. After college, I was envious of alumni who built careers at one company and bought homes to settle down.

Growing up, our family moved frequently because of my father’s job. Then, after college, I married someone in the U.S. Coast Guard. This meant I was forced to adopt the culture of whatever school I attended and, later in life, to find a new job every three to five years.

I complained bitterly at the time about this nomadic life, but now I see it was a blessing in disguise. With each relocation, I learned skills outside my comfort zone that likely would have eluded me if I’d stayed in one place. And I met new, highly talented people who served as mentors—and still do.

Through my exposure to new industries, people and places, I became a better professional. A better person, too.

Our cover story talks about understanding executives’ perspectives to get buy-in for your security programs, particularly cloud solutions. Another article takes a more tactical approach to cloud data sprawl. And, for something a little different, an (ISC)² member reflects on all of the non-technical skills that led to his success as a security professional.

I hope that with member-generated articles like these, you, too, are able to up your game and step outside your comfort zone, whether you intend to stay in one place or not.

Anne Saita, editor-in-chief, lives and works in Southern California.

ANNE SAITA
asaita@isc2.org

ADVERTISER INDEX
For information about advertising in this publication, please contact Tim Garon at tgaron@isc2.org.

CA Technologies.................. 2
(ISC)².......................... 3-4
Black Hat.................. 7
(ISC)².......................... 9
ISACA.................. 15
(ISC)².......................... 29
Capella.......................... 31
Twirling Tiger Press........... 33
(ISC)².......................... 34

© Rob Andrew Photography

www.infosecurityprofessional.com
Use code iSc2BR2 to save $200 off Briefings
SURPASSING EXPECTATIONS

(ISC)²’s new chairman reflects on how much we’ve grown as an industry and organization

About 28 years ago, members from different organizations gathered in a conference room next to my office at Idaho State University to start developing a unified certification model for information security professionals.

We gathered materials from each organization to create what would become the Common Book of Knowledge, or CBK. More meetings followed about how to establish the organization now called (ISC)², and I remember one early meeting where we asked how we’d know if all this work was worth it. Someone quickly crunched numbers and determined if we had 500 to 1,000 people certified, the organization would be a success.

Today, (ISC)² has provided career-enhancing credentials to more than 100,000 professionals across the world. And I have had the good fortune to be part of the organization—initially as a co-founder and today as a unanimously elected chairman of its globally diverse governing Board. The Board sets strategy and has a fiduciary responsibility to members. We also want to make sure members get the most value possible from their membership.

Today, (ISC)² has provided career-enhancing credentials to more than 100,000 professionals across the world. And I have had the good fortune to be part of the organization—initially as a co-founder and today as a unanimously elected chairman of its globally diverse governing Board. The Board sets strategy and has a fiduciary responsibility to members. We also want to make sure members get the most value possible from their membership.

I’m probably the oldest board member at the moment; however, I’m also an agent of change. As a university professor and associate dean, I am surrounded by young people who are demanding that our curriculum is both relevant and current.

In the past decade, (ISC)² has added new certifications and become a growing global organization with regional offices worldwide. Our examinations are offered in eight different languages. We are constantly considering new certification programs, updating existing ones and CPE requirements to ensure our certification holders remain competitive.

In the near future, you’ll see us, particularly through the (ISC)² Foundation, provide more outreach and support to minorities, including community college, undergraduate and graduate students studying science, technology, engineering or mathematics. This helps to ensure their successful transition into the security profession.

The demand for people in our profession is enormous. I witness this daily through my work as a professor and the strong recruitment of my IT security graduates.”

The demand for people in our profession is enormous. I witness this daily through my work as a professor and the strong recruitment of my IT security graduates.

Some 28 years ago, I could not have envisioned that (ISC)² would be as successful as it is today. Now I know it will be even greater going forward.

I am a firm believer that if you’re not changing, you’re dead. We have to keep moving and listening to our membership and to our industry. In return, I encourage each of you to do what you can to make sure that as individuals and as an industry, we continue to be heard by being active in the profession and community, through our chapters and other membership activities.
It takes a **FULLY TRAINED TEAM** to ensure that your **ENTIRE ORGANIZATION** is secure.

Download to learn more at cert.isc2.org/infosecpros.

Visit (ISC)² at **RSA – Booth 108**
NEW (ISC)² CLOUD SECURITY CERTIFICATION

The CCSP® demonstrates competence in managing security in cloud computing environments

FOR INFORMATION SECURITY and compliance professionals seeking to show their competence in cloud security environments, there’s a new (ISC)² credential on the horizon: the Certified Cloud Security Professional (CCSP)®.

Developed in partnership with the Cloud Security Alliance (CSA), (ISC)² plans to make the new international credential examination available beginning July 21. The certification addresses the market demand for knowledgeable cloud security professionals who are tasked with protecting business data and infrastructure in the cloud. CCSP is ideal for those who want to differentiate themselves in the information security market by validating their skills with the most reliable indicator of overall competency in cloud security.

“The CCSP arms professionals with a widely recognized measure of their competence in cloud security.”

Currently, there is no vendor-neutral, advanced security credential that confirms a professional’s skills and competency in cloud security, specifically with regard to best practices for security architecture, design, operations, and service orchestration. The CCSP arms professionals with a widely recognized measure of their competence in cloud security. This provides a valuable differentiation that promotes their cloud security knowledge, skills and experience and instills confidence in them among existing and prospective employers, as well as the industry in general.

The program draws from a comprehensive, up-to-date global body of knowledge that ensures candidates have the right cloud security knowledge and experience to audit, assess, and secure cloud infrastructure environments. Candidates must have at least five years of full-time experience in information technology, including at least three years in information security specifically and one year in cloud computing. Because CCSP builds upon many of the areas covered by CSA’s Certificate of Cloud Security Knowledge (CCSK) in order to provide a deeper set of knowledge and competency, those holding the CCSK certification may waive the one year experience in cloud. It requires practical knowledge and skills covering a broad set of cloud security capabilities and helps confirm candidates’ competence, thereby validating their practical knowledge applicable to day-to-day responsibilities.

The professional credential encompasses the following:

- Exam and testing standards that comply with ANSI requirements
- Legal commitment to the (ISC)² Code of Ethics
- Endorsement from appropriate (ISC)²-certified professionals
- Commitment to continuing professional education

All of these requirements provide employers with increased confidence that CCSPs are qualified and committed to tackling the cloud security challenges of today and tomorrow. To learn more about the new credential program, visit www.isc2.org.
NEW ONLINE TOOL HELPS MEMBERS MANAGE VULNERABILITIES

Vulnerability Central is the first module in a larger portal

ISC² MEMBERS NOW have a new tool to help corral vulnerabilities and published threats found throughout the Internet. Vulnerability Central is powered by Cytenna’s tool, ThreatRank, which is the first module of a larger Security Central portal. New modules are scheduled for release in the coming years.

With Vulnerability Central, system administrators and other information security professionals can:

- Check in to see the latest vulnerabilities and threat reports from around the globe in one place
- Receive early notification of vulnerabilities to be better prepared to respond
- Research and prioritize detailed vulnerabilities, which are categorized based on criticality
- Filter vulnerabilities based on the type of assets being managed, such as showing Microsoft and Cisco vulnerabilities, but not Unix
- Provide a quick resource for published threat reports
- Follow links to relevant information security news articles

“The power of Vulnerability Central is using proprietary, state-of-the-art algorithms to aggregate, categorize, and prioritize vulnerabilities affecting tens of thousands of products, then putting them all in to one place. This can save a lot of time for our membership that need, or can use, this data,” said Erich Kron, CISSP-ISSAP, HCISPP, (ISC)² director of Membership Relations and Services.

The tool uses Single Sign-On to provide the authentication for the members using their (ISC)² member login (meaning no extra accounts to create/manage) and to link them with their profile. For more details, please log in to Vulnerability Central using your member login credentials at vulnerability.isc2.org.

TOP TWO challenges cited by businesses new to the cloud:

- Security
- Compliance

71% of IT pros believe that their cloud service providers WON’T alert them to a data breach that involves customer data

SOURCE: March 2015 Seclore survey
YES, GRANDMA, IT IS SAFE

When my 83-year-old grandmother asked me a few months back whether our Skype calls were encrypted, I realized that encryption was no longer a resident of the nerd-only realm and has graduated to become a household concept.

Working in cryptography, I discuss terms like Elliptic Curve Cryptography and forward secrecy on a daily basis, so to help my fellow PKI people, and with the help of the graphics design studio CreateHive, I’ve created a poster that summarizes some of these concepts, and illustrates the structure of a Cipher Suite.

I sent this to a few friends at work and placed a PDF download on my personal blog (http://www.isitsafe.us). I figured a few people might want the poster, but imagine my shock when less than a week later, there had been more than 1,700 downloads.

This suggests more than grandmas want to understand better—or help translate to users—cryptography basics. A subsequent presentation I gave on the same subject...
GLOBAL SPOTLIGHT: (ISC)² ATLANTA CHAPTER

ATLANTA CHAPTER LENDS A HAND AT SECURITY CONGRESS

IF YOU ATTENDED last year’s (ISC)² Security Congress, there’s a good chance you met members of the Atlanta Chapter. They served as session moderators, introducing speakers on a wide variety of topics at the Georgia Congress complex. They also helped distribute and gather evaluation forms at each session and, in general, augmented staff during the annual event.

(ISC)² Atlanta was established in February of 2012. With a starting base of 20 members, the chapter has grown to nearly 200 members in the three years since the Chapter’s founding. Mikal Haas, the Chapter president, attributes the growth to “being active in the IT security community.”

The Chapter’s activities pay dividends, as Haas notes in two of their recent efforts. The 2014 (ISC)² Security Congress brought in thousands of attendees and the opportunity for making connections. The Chapter’s participation in the 2014 Secure World Expo also had rewards: “We had a booth, and we had a user group meeting that was one of our more successful meetings to date.”

In 2015, the (ISC)² Atlanta Chapter became part of the advisory council of the Atlanta Interface Conference, joining national and community-based organizations in this annual presentation of the latest news and developments in information security and technology.

The Chapter, in keeping with the (ISC)² mission to educate the next generation of information security professionals, is partnering with Gwinnett College to bring the (ISC)² Global Academic Program to campus. Haas sees this as a win-win: “I think this has a lot of upside to both Gwinnett College and the (ISC)² Atlanta user group.”

—Deborah Johnson

Erez Benari is an (ISC)² member and senior security specialist, working within a Microsoft IT group’s Identity and Access Management team. Previously, he has been part of the ISA server development team and worked on other Microsoft products such as UAG and DirectAccess. He also spent time as a program manager for IIS and Azure Websites.

Encryption software such as Microsoft’s SChannel (which is used by most programs running on Windows clients and servers) can be configured to give preference to different parts of the cipher suite. For example, even if your server is too old to upgrade to Windows 2012 R2, you can still use Group Policy and tell the server to give preference to more secure key exchanges, ciphers, hashes, etc.,—all without spending a dime.●

“…Having an old server or running an old OS doesn’t mean you’re stuck with old encryption technology.”

●

Return to Contents

Field Notes

CONTINUED FROM PAGE 12
drew a huge crowd.

For me, the unexpected demand is less about remembering the difference between DHE and ECDH than it is about understanding that having an old server or running an old OS doesn’t mean you’re stuck with old encryption technology.

—Deborah Johnson

CONTINUED FROM PAGE 12
FROM THE TRENCHES: MAKING THE SALE

JUST AS MANY of us have been saying, “Security is everybody’s job,” a wise man once said, “Everybody is in sales.” The truth in these two maxims is nowhere clearer than during a company’s information security budgeting process. Recently, being fresh in my new role, I inherited a budget based upon the previous year’s spend in security and was asked to rewrite it. In many ways, I discovered, this was less of a writing exercise and more of an archeological endeavor.

For each line item, I had to uncover the “why” and “how” for every operational expense and projected capital project. This meant reaching out to various stakeholders in the lines of business, as well as to a large contingent in IT. I then had to evaluate the merits of each budget item against the corporate strategic plan and the broader security needs of the enterprise to add the context I needed beyond the anecdotes gathered.

In many ways, this is similar to a seasoned salesperson trying to get you to purchase their next big product. A good salesperson does the legwork to understand your business—not just where their product might fit, but to gain appreciation for your business at a deeper level. They are also adept at cultivating relationships across your IT teams and throughout your business.

Stealing from the sales playbook, I began to formulate a strategy for the coming year. From staffing levels to planned projects, nothing was sacred. For each and every dollar spent, there had to be a corresponding link to the broader corporate objectives. Some would call this a “business case,” but it is less about the actual numbers and more about the impact. I had to tell a story. A very interesting story, with a broad audience.

For each stakeholder, or groups of similar stakeholders, I had to weave a narrative around my projected 2015 activities that they would find compelling and worth supporting. For each level of the organization so that they can see clearly how my efforts align with their own goals and to rally them around my program, making security (at least partially) their job.

It is now time to further refine my messaging for each level of the organization so that they can see clearly how my efforts align with their own goals and to rally them around my program, making security (at least partially) their job.

As I continue to host and moderate (ISC)² webinars, you’ll likely hear a slight shift in my line of questioning. It isn’t just going to be about the problems and their corresponding solutions but also about how to articulate the benefits of solving that problem at that time. I’ll be asking the panelists how they developed the support for their projects and how they overcame the hurdles to gaining the buy-in they needed. Essentially, I’ll be asking them how they came to be a security salesperson.
“I EARNED THREE ISACA CERTIFICATIONS. EACH HAS BEEN CRITICAL TO MY SUCCESS.”

— OPEYEMI ONIFADE, CISA, CISM, CGEIT
PRACTICE LEADER, AFENOID ENTERPRISE, LTD
ABUJA, NIGERIA
ISACA MEMBER SINCE 2010

Becoming ISACA-certified showcases your knowledge and expertise. Elevate your career and gain the recognition you deserve with ISACA certifications—register for an exam today!

Register at www.isaca.org/SeptExams15-isc2

ACCOMPLISH MORE

REGISTER FOR A 2015 SEPTEMBER CISA OR CISM ISACA CERTIFICATION EXAM TODAY!

Early Registration Deadline: 17 June 2015
Final Registration Deadline: 24 July 2015
Register early and save US $50!

UPCOMING CERTIFICATION EXAMS*:
12 September 2015
*Early Registration Deadline: 17 June 2015
*Final Registration Deadline: 24 July 2015
*Register early and save US $50!

*CISA®, CISM®, CGEIT® and CRISC™ exams are also available in December—registration opens soon!

www.isaca.org/SeptExams15-isc2
TRANSPARENCY AND TRUST DRIVE CLOUD SUCCESS

BY JIM GOLDMAN AND J.J. THOMPSON

WHEN IT COMES to a company’s cyber well-being, the assumption is that the executive board and the IT team, though coming from different directions, have the same goals in mind. While the board is concerned with the impact of security issues on reputation financials, the CISO is selecting, deploying, and managing the capabilities to address these board-identified risks. So what could go wrong? Plenty.

BUYING INTO THE CLOUD CAN SEEM LIKE A FISCAL WIN FOR A COMPANY’S BOARD—BUT IF THE EXECUTIVE AND IT UNITS ARE NOT ALIGNED, THE ENSUING STORM COULD SPELL DISASTER

PHOTOGRAPH BY PAUL D’ANDREA
When decisions are made in the boardroom without the participation of the CISO, key messages are lost. Nowhere is this disconnect more apparent than in the discussion about cloud services. To the company’s executives, the “cloud” is a cost-effective business service but a costly IT investment. The CISO is then presented with a “cloud” solution, one which may not be for the company’s benefit.

In this article, we outline common board perspectives regarding cloud services and offer approaches CISOs—and those who aspire to the position—can take to gain the board’s trust and manage their expectations about the cloud. We also highlight three case studies in which the trust factor directly impacted the outcome and then provide methods to create trust within your organization.

HOW BOARDS VIEW THE CLOUD

According to a 2013 Forrester Research survey, 50 percent of businesses in Europe and North America identify security as the No. 1 reason for not adopting cloud computing. This trend continues, based on service delivery architecture planning we have participated in for 2015. The key is to isolate those considerations that create the lack of trust and develop countermeasures.

Building an approach and a communication plan is key to securing adoption of cloud capabilities. A previous article in this magazine on managing cloud expectations (“Is There a Cloud Hanging Over You?”, March-April 2014) outlined five key attributes expected by executives and the board: visibility, intelligence, resource throttling, real-time scalability, and outcome-based metrics.

50 percent of businesses in Europe and North America identify security as the No. 1 reason for not adopting cloud computing.

—2013 Forrester Research survey

These same components can be used by the CISO/CIO to gain the confidence of the board that you are managing your cloud solution. In addition, it is vital to research the positions of your key stakeholders impacting your cloud security strategy—for or against—and determine how to overcome their concerns.

Here are some common opinions about the cloud, both positive and negative, that we’ve identified through our interactions with clients in Q4 2014.

CASE STUDY #1

IPO Security Program Preparation
A Silicon Valley-based firm weighs on-premise vs. cloud improvements

A n information security technology firm had hired a new VP of IT as it prepared for its Initial Public Offering (IPO). The first question the board presented to him was what he planned to do to improve their security capabilities, as it was critical that every precaution be taken to avoid compromising data or software updates to customers around the world.

After a brief statement on his high-level approach, the board agreed with his plan and let him know that he would have their full support. Based on his reputation and his effective communication about his plan, they placed their trust in him.

The architecture for the required capabilities would lead to the critical decision: on-premise, public or hybrid cloud variant?

Founders and internal key influencers were completely against the concept that protection of sensitive data would require the data to leave the premises due to the simple fact that they themselves are a security company and did not want to relinquish trust. Trust was too risky, as it could cause irreparable harm should a third party fail to deliver on the transitive trust the customer had placed in them.

As a result of these factors, it was decided that the security program would be wrapped around fully on-premise managed capabilities. In this case, trust could not be transferred to the cloud.

—Source: Rook Security
Positive attitudes toward the cloud

- The cloud adds value to existing offerings
- We can test new ideas with less capital expenditure and decrease time to market and time to scale
- Improved ability for business process transformation with tech enablement
- App teams are able to move faster, with improved ease of integration
- Configuration and management of certain categories of apps are best done by external industry experts, rather than by internal IT resources

Negative attitudes toward the cloud

- High risk in terms of security and privacy
- Internal teams haven’t succeeded with securing on-premises; how will they be successful in the cloud?
- Should we trust an “outsider” to do a better job of managing the infrastructure/applications/security than us?
- Numerous flavors of “cloud” lead to uncertainty and risk avoidance

The additional degree of separation demands increased oversight of third-party hiring practices and operational processes

Boards want to realize the positives of cloud services, but they struggle with trust issues and fears surrounding the negatives. It’s a classic case of risk vs. reward. The fundamental operational question is, “How do we tip the balance away from risk toward reward?”

MANAGING BOARD EXPECTATIONS

The approach that is right for your organization is based on: 1) current fires, 2) precedents, 3) current politics, and 4) the executive roadmap. Using that information, there are two approaches to communicating to the board about the cloud:

Proactive strategic roadmapping

Work with senior executives to determine the board’s concerns regarding cloud capabilities (a good starting point is listed above), identify your plan, and then identify where there may be gaps.

Treat the board as your customer and your planned offering as the product they will consume. They want to...
know in clear, concise terms:

- What problem you’re trying to solve
- How the (cloud) solution helps
- Where issues may arise
- Whether there’s a consensus among key stakeholders
- That you have a plan in place

Tools are available that can simplify and delineate the challenge. One tool provides a template to list objectives, goals, the current state, and immediate actions (see Figure 1).

Another provides a roadmap template to illustrate the challenges and the routes to solutions (see Figure 2).

**Reactive Rapid Response Plans**

While we would all like to anticipate and control the message, all too often board or executive team members react uniquely to a challenge. They tend to frame problems in a manner that makes sense to them, often relying on gut instinct and precedent; whereas, IT gives more credence to empirical data. Lately, this gut-wrenching anxiety is strengthened by media reports about security breaches that send the security executive into response mode, a situation with which many CISOs are familiar.

In a reactive mode, the key difference is that the starting point is already established, and it’s up to the CISO to elicit the key components: What is the concern/question? Who was the originator? Why/what was their key concern?

This last question—addressing the root cause for concern—is where technology-led security professionals can fall short. They take a board’s suggestions or instructions literally without asking enough questions to determine whether this is actually the proper course. This is because the technology is in their comfort zone, while developing deeper conversations with peers or superiors is not. For example, if the message is brief and tactical, then more discovery should happen before racing off to formalize the solution.

Regardless of the approach, there are varying levels of success with adoption of cloud capabilities.

Illustration of a visual security roadmap used for executive communication.
A 

AN INTERNATIONAL INCIDENT arose, requiring immediate “boots-on-the-ground” outside of the United States while working in parallel stateside to collaborate on reputation management and related messaging. An additional layer of complexity required assistance in managing the expectations of client executive teams in legal, risk, and security. The nature of the incident, beyond technical forensics work, demanded timely and tight cross-departmental collaboration with leaders and staff in key areas, including IT, security, human resources, project management, legal, and finance.

Instead of following the usual hard-core security executive-led approach of “disclose nothing and delay,” the CIO decided to be transparent, facilitate collaboration, and achieve buy-in with their client’s executives.

The CIO provided clearly defined expectation management and transparency, with strategic and tactical input from the CISO and CPO. Specifically, this included starting with the critical questions that were being asked and backing into what the assumptive steps needed to be to resolve those questions, the associated anticipated work effort, and anticipated challenges.

This level of transparency shared at the onset of the incident allowed the customer’s CPO and general counsel to collaborate on the incident response strategy, tactics, and timing. This was the catalyst for increasing trust with the customer, as these details in planning are usually concealed from customer executives.

In fact, the resultant testimonial served as reinforcement that proper incident response can have a positive goodwill effect, stating that the “strategic, methodical, and transparent” approach not only re-established trust, but also forged additional levels of higher trust than previously existed.

—Source: Rook Security

Trust Through Transparency, Especially in IR
A service provider opts for transparency to recover from an international incident

TRUST VS. SECURITY: MORE THAN JUST SEMANTICS
Within an organization, security is often inwardly focused—toward its people, technology, and information systems, while trust is often outwardly focused—reflecting the relationship of customers, vendors, or partners that interact with that organization. Sometimes, the two conflict.

For example, one could reasonably conclude that a given organization’s information systems were secure based on a knowledge of its security controls, but that would not necessarily guarantee that the organization could be trusted by a third party (consumer, vendor, partner) who might be looking to do business with that organization. An illustrative quote might be, “I believe that company’s systems are secure, but I still don’t trust them.”

In the event of a reported security breach, a customer of the breached company would have expectations in terms of responsiveness, frequency, and transparency of communication, whether or not those expectations are spelled out in contracts. Failing to meet those expectations, whether known beforehand by the breached company or not, will result in an erosion of trust between the customer and the company.

In the context of the online business world, Integralis, an information security and risk management company, found that people who regularly bank and shop online do not necessarily trust those online companies.

In a 2014 Forbes article, “Five Lessons for Every Business from Target’s Data Breach,” three of the five lessons (communicate the problem pronto, be ready to respond to your customers, and rebuild trust) had to do with trust rather than security.

MORE THAN 70% of survey respondents indicated they preferred a managed security service to protect their cloud workloads

SOURCE: Alert Logic-sponsored third-party survey of 400 IT/security decision-makers who have deployed, or are actively planning to deploy, workloads in cloud environments
A Fortune 500 company was using a mainframe-based Collaborative Lifecycle Management environment for development of firmware to be downloaded onto embedded controllers. Because this company had multiple global operations, configuration and patching, as well as version control, had proved difficult. Due to the complexity of the software, performance was sub-optimal, and the company felt it was not getting the optimal benefit from the software.

The Collaborative Lifecycle Management software environment contained source code for the firmware to the company’s embedded controllers, making it essential that this software not be hosted on a typical multi-tenant public SaaS cloud. By offering a virtual private cloud solution with dedicated VLAN (virtual local area network), known as a hybrid cloud, the company was satisfied with the level of trust communicated by the cloud service provider.

As a result of the numerous instances of the Cloud Service Provider managing this Collaborative Lifecycle Management software, higher levels of expertise in configuration, patching, upgrades and performance tuning were now available. This led to increased trust between the customer and cloud service provider and to more opportunities for deploying other software in virtual private clouds.

The trust architecture portrays the complex building and communication of trust between a cloud services provider, its customers, and the boards of those customers.

Cloud service providers must be transparent and truthful in detailing their capabilities, integrity, agenda, and track record to customers. For their part, customers must provide feedback to the cloud service provider regarding any concerns they have regarding these key elements of trust. The transparency continues as the customer’s IT or security organization communicates to the company’s board in order to gain their trust, and they must, in turn, welcome the board’s feedback regarding any issues of concern related to trust.

But before a company and a cloud service provider can come to terms, the issue of trust between CISOs and executive boards must be resolved. Boards generally want to adopt cloud services, but they may need convincing, and it will take a trusted IT executive to see that through. Whether it’s through proactive, strategic roadmapping or reactive rapid response plans, CISOs should take the lead and use the approach that works best for their organization.

James Goldman is chief trust and security officer at CloudOne.

J.J. Thompson is a security executive at Rook Security and specializes in strategy, response, and next generation security operations. He is a previous writer for InfoSecurity Professional magazine.

Patrick Heim, head of trust at Dropbox, contributed to this article.
LIKE THE TYPICAL TEENAGER’S BEDROOM, FINDING—LET ALONE MANAGING—ALL THAT SENSITIVE INFORMATION STORED BY CLOUD SERVICE PROVIDERS MAY APPEAR ELUSIVE. IT’S NOT.

ILLUSTRATION BY ENRICO VARRASSO

DATA STORED WITHIN the cloud, in the universal sense of the term, is like a teenager’s bedroom—it can get messy. And like frustrated parents who continually call on recalcitrant teens to clean up all that proliferating “stuff,” security professionals seeking the same from users often meet resistance or even rebellion. People just don’t have time in their busy schedules to manage all of the data they’ve stored in third-party cloud services.

Cloud service providers will eventually resolve many third-party or hosted cloud security issues, such as common contractual issues and alignment with standard control sets.

In the meantime, the data sprawl problem that currently exists can only be solved by the customer, and the solution requires more than technical controls. It requires organizational maturity and focused attention—from everyone, not just IT.

For many organizations, the proliferation of cloud-based services has resulted in organizational data being transmitted, processed, and stored by numerous unrelated third parties. The situation quickly becomes uncontrollable, with sensitive data spread out across a large
number of external parties, with little centralized tracking and management.

The fundamental question is whether your organization can easily identify every third party that stores, processes, or transmits data for which your organization is financially accountable.

**DETECTING/MONITORING INFORMATION FLOWS**

The first step is to treat information like an asset and create a comprehensive, centrally managed inventory of all (organization-wide) third parties that store, process, and transmit information for which the organization is accountable.

Unfortunately, organizations often struggle with maintaining accurate physical asset inventories, despite the abundance of tools available to assist in those processes. Information asset inventories are even more difficult to maintain, given that the processes are largely manual, and automated technical controls are not available or not widely deployed.

The information inventory must facilitate reporting and analysis (whether stored in a database, spreadsheet, or application) and should contain relevant attributes for each third-party instance.

Suggested attributes include:

- Cloud Service Provider (CSP) name
- CSP contact information
- Service model (e.g., SaaS, PaaS, IaaS, STaaS)
- Contracting business unit
- Financially accountable information owner
- Information custodian
- List of every data element
- Applicable regulations and contractual requirements
- Reason/justification for using cloud service

Some organizations will require each business unit to maintain its own inventories, while others will delegate responsibility to the IT or information security departments. In larger enterprise organizations, a central inventory managed by an entity that has enterprise scope (IT or information security) provides the best comprehensive view. The input sources for the inventory vary in each organization but generally should come from central teams that have engagements with, and awareness of, all sourcing agreements.

For example:

- **Purchasing and Legal** – These entities are involved in the purchasing and contractual processes.
- **Accounting/Finance/Treasurer** – Standard back-office functions may be able to identify financial transactions with CSPs.

- **Human Resources (HR) and Payroll** – These functions have the greatest interaction with sensitive employee data and its usage.
- **Information Security and IT** – These functions are often involved in the design and architecture of new solutions, including those that do not require internal infrastructure or integrations.
- **Cloud Services Brokerage** – Brokerages are still gaining traction in the industry; however, the brokerage should be the source of information for all cloud projects in organizations where implemented.

Be aware that those processes are often manual and prone to bypass (i.e., the purchase of inexpensive public cloud services using a business or personal credit card to bypass standard purchasing and contractual processes).

Where possible, organizations should strive to implement technological controls to monitor, detect, and block data being transmitted to third parties. This is especially important in organizations that have a large user population or many remote users. *(See sidebar on p. 24 for a list of potential technical controls.)*

**FICKLE USERS AND APP EXTENSIONS**

One of the biggest challenges is the removal of stale data from cloud storage due to fickle usage.

For instance, users with immediate needs may store data in any available cloud service or decide on a new “flavor of the month” cloud storage solution. They also may change jobs or be terminated, resulting in an “orphan” account. The aforementioned controls (see “11 Ways to Gain More Control...,” p. 24) can be used to monitor and track cloud service usage, facilitating detection of stale external data repositories that are lingering long after active usage has ceased. This activity is critical. The data may still have value, and the account may still be using credentials that were compromised in a breach at another service (i.e., former employees who’ve forgotten they have an account and did not change their password).

Another challenge is the plug-in/extension/integration dilemma. Applications, particularly SaaS applications, may support third-party extensions. For example, Salesforce.com is designed as a platform and has over 2,500 apps available through the AppExchange marketplace. Some apps will transmit data to the app developer’s data center for processing and possibly storage before transmitting the data back to Salesforce.

The risk analysis process needs to com-
1. Network Data Loss Prevention/Perimeter Firewall/Intrusion Detection System/Intrusion Prevention System – Any combination of these technologies can detect data leaving the network, especially when deploying “next generation” firewalls. However, these controls require a strong perimeter and may be easily bypassed in organizations with large remote user populations or heavy Bring Your Own Device (BYOD) usage.

2. Web Proxies – Web proxies can prevent users from accessing prohibited sites, but in many organizations, proxy implementation only covers internal users.

3. External Internet Gateway/Web Proxy – One solution to the remote user gap is to require organization-managed devices to connect to organization-managed proxies for all Web connectivity, even when those devices are off-network. With these controls in place, proxy rules will apply to user activity regardless of network location. However, additional controls are required to prevent users from copying data to an unmanaged computer (e.g., personal computer on their home network).

4. Host-based DLP/IDS/IPS/Firewall – Host-based controls close many of the gaps from their network-based counterparts, but tuning and management can be unwieldy, depending on the size and diversity of the organization and its business processes.

5. Host-based Website Blocking/Activity Logging – Most anti-malware suites include functionality to blacklist or whitelist Websites based on reputation rating and other criteria. This functionality complements Web proxies and may be less expensive than managing an externally accessible Web proxy.

6. Automated Endpoint Software Inventory/Application Whitelisting – Either of these controls can be used to scan endpoints for installed remote storage clients and other signs of cloud app usage. Organizations with strict endpoint requirements can always prohibit installation of unapproved software, but that requirement will be too restrictive in many organizations.

7. Require Virtual Private Network and Prohibit Split Tunneling – For organizations with stringent control requirements, one option is to require mobile device network connectivity only via approved VPN connection. Forcing all remote users back to the organization’s infrastructure extends internal controls to external devices but at the expense of network bandwidth and increased network device utilization.

8. Rogue System Detection/Endpoint Identification – Controls 1-7 are most effective in organizations that prohibit BYOD. Organizations with a flexible BYOD program must consider whether to deploy controls to identify personal devices and enforce endpoint controls on them. These tools are most effective when users are on the organization’s network. Organizations with Internet-accessible applications or a large number of remote workers will have more difficulty restricting users from storing data on their personal devices.

9. Social Content Monitoring/Deep Web Scanning – These detective controls can uncover sensitive data residing on externally accessible systems, but they cannot detect data that is password-protected or requires authentication.

10. Security Information and Event Monitoring – Many technical controls produce logs that require inspection and analysis. Technical controls provide little value if the log review process is inadequate. Organizations managing a large number of devices or implementing multiple controls require a SIEM system to assist with log management and review.

11. Promote Preferred Providers/Solutions – For infrastructure solutions (e.g. IaaS, BaaS, STaaS), organizations should consider restricting business units to contract with a limited number of preferred CSPs. If organizations do not build their own solutions (i.e., private cloud), they should consider developing a framework architecture to facilitate leveraging internal controls and infrastructure with external CSP services (e.g., leveraging federated identity management system for authentication with external applications and systems; using internal key management infrastructure to implement user-managed encryption with external storage providers; passing all traffic through perimeter controls; extending internal domain to the cloud environment).
prehend the risks associated with any Salesforce apps the organization’s employees may be using, along with standard downstream risks (e.g., third-party suppliers to the app developer). And, without a centrally managed vetting process, organizations may be unaware of all of the third-party apps integrated into their Salesforce instance.

A related challenge is tracking the functionality and data elements being used with any cloud solution, especially SaaS applications, which may frequently deploy additional functionality.

“Without documented guidelines and disciplinary actions, it is impossible to hold users accountable for their actions related to data storage, processing, and transmission.”

New software releases could require access to additional data elements or use of existing data elements in a different way. Security and privacy vetting processes for cloud-based solutions should include periodic updated assessments that include validation of functionality and data element usage.

One process for SaaS applications is an annual review of any official notes for new software releases to the SaaS application that were deployed in the past year. SaaS providers may require customer approval prior to migrating them to new versions (especially with major releases), and a recommended best practice is to require additional internal security and privacy reviews prior to approving that migration. However, tracking functionality changes is difficult, as security and privacy assessors are often not application users and could easily miss subtle changes, such as new reporting functionality that aggregates data differently.

POLICY AND STANDARD: PROVIDING THE FOUNDATION

None of these controls are effective without supporting policy statements.

Minimally, information security policies and standards need to include requirements for information classification and handling, a framework of requirements for cloud-based activities, and statements indicating that cloud-based environments are identical to internal IT environments when considering applicability of information security requirements. Appropriate disciplinary actions also need to be included, with support from business leadership and HR.

Changes to policy and related disciplinary actions must be communicated through awareness and training programs to educate users on cloud usage. Training is especially critical for “young” employees (under the age of 30, according to some analysts), who were raised in a world that was largely “always on” and cloud-connected.

Without documented guidelines and disciplinary actions, it is impossible to hold users accountable for their actions related to data storage, processing, and transmission.

GREAT EXPECTATIONS

Expect data sprawl issues to exist for the foreseeable future. There are too many influential factors, particularly user behavior and organization size, to do otherwise. Many organizations have launched extensive user awareness and training programs that include information classification and handling, but improving user behavior through training programs is difficult. Users tend to have difficulty applying examples from one scenario more broadly to other similar activities.

Organization size also contributes to its ability to contain data sprawl. Smaller organizations have smaller budgets, but they also have fewer users to manage. Large enterprise organizations have larger budgets, but they face barriers in the complexity of managing large numbers of users across diverse business units. Regulatory requirements provide a lever to justify spending, but not all sensitive data is regulated, especially in organizations that invest heavily in research and development or have other sensitive service or product documentation.

As long as cloud-based services continue to provide business benefits (such as speed, agility, pricing), they will be seen as attractive solutions. Organizations need to strive to understand where their data resides, who is managing it, and how it is being managed. The first step is maintaining a comprehensive information inventory detailing all third party transmission, processing, and storage. In many organizations, data sprawl cannot be contained without some implementation of technical controls.

And unlike that proverbial teenager’s bedroom, security professionals can’t just shut the door and walk away.

AARON SANDERS, CISSP, is a senior IT risk analyst for Xerox Corporation, located in Rochester, NY. He can be reached at aaron.sanders2@xerox.com.
Yes, It Is Your Business

An (ISC)² member explains how you can be more effective by embracing the non-technical side of security

by Tony Vargas

Hirty years ago, I remember getting games for Christmas and spending all day trying to install the programs via floppy disks before configuring them on my computer. Those days, PCs were simpler and not always connected to a network. As time progressed, that “computer hobby” turned into a security career.

Today’s computing world is no longer focused as much on games people play as it is about what business, social, and economic problems it can help solve (or create).
In my career, I’ve worked at large companies, medium-sized companies, startups, and non-profits. I’ve learned different and valuable lessons from each experience. I’ve also been an individual contributor, manager, and advisor. Each role has had different challenges, and I’ve found that experience in one role has helped me in others. I’ve also found common themes in excelling in all these roles. Primarily, if you want to move ahead (or just gain entry) in your career, you need to know how best to listen to others, be patient, speak well, persist, collaborate, and be a team player, even a team leader when the occasion arises.

LEARN TO LISTEN ACTIVELY
As an engineer and security professional, I’ve found listening to be among the most useful tools to being successful. Truly listening can be extremely difficult, mainly because we aren’t used to giving someone our undivided attention for more than a few minutes. But, by clearing away the distractions and actively engaging in a conversation, I usually learn something new.

Listening also allows me to gain a new perspective or perspectives on an issue on a more holistic level. I am able to leverage the experiences of others and maybe even find a new opportunity for the business. Listening also creates stronger relationships between individuals. Nothing makes as good an impression as asking thoughtful, on-target questions and accurately summing up the conversation and action items before departing.

I used to give operational reviews to senior management for a multi-billion-dollar product line. This role gave me the opportunity to work with more than 400 people throughout one product group. By listening actively to group members, I gained a clear understanding of some technical issues that the organization needed to address. For one project, by truly talking through a task, we were able to reduce the time it took by more than 80 percent. On another project, we improved production by more than 300 percent. I was able to help by listening, making sure I fully understood, and then suggesting and helping implement the technical fixes within my purview.

PATIENCE IS A VIRTUE
Another tool that I have found to be important is patience, and this is a real struggle for me. As an engineer and security professional, I have an inherent tendency to want to fix issues as quickly as possible, yet I also find that fixing something quickly is not always best.

The proverbial “dive and catch,” where you save the day by fixing the most pressing incident at hand, can feel rewarding when an event first occurs. But applying a fast fix also can create problems strategically and doesn’t scale well (it leads to burnout, and the root causes of issues are never addressed). Business processes are not always able to change instantly, especially in larger organizations. For instance, after a group of us decided that we wanted to create a 501(c)3 non-profit, it took more than 16 months for the paperwork to get processed. There was nothing we could do but wait.

That waiting period made running the organization very difficult because the non-profit was not yet approved, and therefore, we were unable to get tax exemptions and provide tax deductions to donors, yet we found that companies and partners were understanding and still willing to work with us (coincidentally, we were lucky, and our non-profit paperwork was approved the first time we applied).

Additionally, patience has been helpful because all individuals involved in the non-profit were doing so in addition to their full-time jobs. People have life events that disrupt deadlines and put project completions at risk. The key is to have contingencies and trust that those asking for more time will come through for you. They usually do.

Patience also has helped me think more strategically and holistically about security and business issues in general because it has forced me not only to examine the immediate issues and end goals but all the possible scenarios in between.

Another area where I find patience helpful as a security professional is in the area of influence. For instance, when I’ve helped implement some security policies in the past, it has sometimes taken a few years for those changes to gain traction within the enterprise. The policies were just ahead of their time, and the business wasn’t ready for them.

SPEAK UP
Public speaking helped me immensely to become a better professional because it helped me learn how to improve how I communicate. Although I have been speaking internally at companies for some 17 years, in 2011, I started speaking at conferences. I have found that speaking in-house differs greatly from speaking at conferences, particularly in how you respond to audience questions. Each speaking venue can be different and thus can have different capabilities, which can impact the talks. I’ve also learned to evaluate each presentation separately and not to compare them.

One of the best tools that helped me build up my presentation skills has come from volunteering with the (ISC)² Foundation’s Safe and Secure Online program. I’ve learned more by giving Safe and Secure Online presentations to children ages 7 to 17, parents/teachers, and seniors than I have from many other presentations, because during those talks, one has to be much more conscious of the full environment beyond just the slide content.

Making sure that the audience understands how the
technical content on the slides is relevant to their lives can be challenging yet incredibly rewarding. Specifically, delivering (ISC)² Safe and Secure Online presentations has taught me how to change the message I am conveying to meet the needs of a particular audience—on the fly, if needed. Ironically, it has also helped me be a better engineer and security professional because it helped me better understand what issues end-users encounter.

The primary reason I speak, though, is to help others. If I can help someone be more effective at their job through one of my talks, then the talk is successful.

I also like doing panels. Panels allow four to five presenters an opportunity to help the audience. I believe that multiple perspectives regarding a subject are more helpful than just one. Remember: Presentations are about helping the audience, not about enhancing your career.

DON'T GIVE UP
Persistence is also a skill that often is overlooked and under-appreciated.

For most of my career, I wasn’t involved in all aspects of a business such as marketing, sales, accounting, etc. That all changed when I decided to start a non-profit, which, for me, required a steep learning curve.

By-laws and corporation entity types were all new experiences for me, along with knowing the financial and legal implications of each. Determining an organization’s mission in order to determine its corporate structure is also difficult. Persistence—sticking with something despite all those obstacles—is key, especially when issues are not quickly addressed.

Persistence is important because security initiatives are not always top of mind. Sometimes security initiatives take years to garner enough support to move forward. Many times, security initiatives change after receiving support due to funding or resource constraints.

The important thing is to be flexible but firm in your pursuits to improve your organization’s information security posture.

WORK TOGETHER
I’ve long believed that the security profession consists of some of the brightest and most compassionate individuals in the world. This is both a blessing and a curse. Security professionals see things that others do not, but we often are dismissed as spreading fear, uncertainty, and doubt (FUD). We are often tasked with finding evidence of events that have not yet happened just to prove our worth. It is a difficult position to be in, akin to repeatedly running headfirst into a wall.

For many security professionals, these frustrations lead to burnout. A best practice to prevent that is to network with other security professionals and attend security conferences. Not only do you learn about emerging threats and mitigations, but you find kindred spirits who can help you by sharing their own experiences. This type of networking can save your company and maybe even your career.

Teamwork and collaboration also help me stay up to date on trends in the industry. We are typically too busy dealing with the daily minutia to pull back and notice what is happening elsewhere. It is also a good way for me to get different perspectives about various topics, especially in security, where many components are becoming specializations.

Having a diverse network also helps remove obstacles and garner needed support for various security initiatives. I’ve seen scenarios where an individual’s manager resisted a new security policy until someone from another organization was able to help convince the recalcitrant manager that a policy was worth supporting. In fact, most of the successful security policies and programs I have witnessed were eventually adopted because high-level executives from different organizations worked together.

THE ECONOMICS OF SECURITY
One important component I haven’t mentioned yet is economics. Economics play a key role in all aspects of security. Knowing the difference between CAPEX and OPEX expenditures is important, as they have different rules and limits, which have different impacts on budgeting. Knowing the financial health of your organization is important when determining which security initiatives and solutions to address. Also knowing dates of your organizations’ fiscal quarters is important, as it can impact whether someone says “yes” or “no” to a needed purchase.

As all security professionals know, the number of incidents and attacks far outpaces the supply of security professionals in the world to combat them. This means we need to look beyond just the technical issues regarding security; we need to be aware of the business side of security in order to make the kind of contributions to the company that we all envision. I hope that some of the lessons that I’ve learned over time can help other security professionals succeed.

TONY VARGAS is co-founder and CEO of Security Together, a security engineering and consulting firm. Tony is also the chair of (ISC)²’s Application Security Advisory Council and co-founder and chairman of the (ISC)² Sacramento Chapter. In October 2014, he won the (ISC)² President’s Award for his leadership and contributions to (ISC)². In 2013, Tony won the inaugural Cisco Product Security Champion of the Year Award. He was also a Cisco Product Security Champion in 2012. You can find Tony at @tvargasciodb.
From Zero to 60
Advancing the Cybersecurity Workforce

May 14th and 15th, 2015 | Washington, D.C.
Ronald Reagan Building and International Trade Center

Register Now

Keynote Speaker - James C. Trainor, Jr.

As the Deputy Assistant Director of FBI’s Cyber Division, James C. Trainor, Jr. manages all Cyber Operations Sections. Prior to summer 2014, his role included managing all non-Cyber Operations Sections. Previously, he has served with FBI Chicago, New Haven, Boston, New York and Headquarters in criminal, counterintelligence, intelligence, espionage and economic espionage matters. Prior to joining the FBI, Mr. Trainor was a military intelligence officer for the U.S. Army.

Visit the (ISC)² Career Fair at CyberSecureGov

Meet with an Information Security recruiter for career coaching and resume review tips.

Meet face to face with employers with open positions looking to hire!

cybersecuregov.isc2.org | #CyberSecureGov
2015 (ISC)²® WORKFORCE STUDY UNCOVERS A COMMUNICATIONS PARADOX

AMONG THE MORE interesting results of the recently released 2015 (ISC)² Global Information Security Workforce Study is a growing need to build general management skills, specifically the need for strong communications skills.

A significant number of professionals currently focusing on operational responsibilities see themselves moving into managerial positions in the near future, and they view education and certification as a way to support their goals.

Worldwide, 59 percent of the workforce intends to earn an additional certification in the next year, which is impressive given the time and study involved in earning a credential. Even more interesting is that about half of C-level information security professionals intend to earn a new certification in the next 12 months.

Consequently, 90 percent of those surveyed believe their training needs would either increase or stay the same in the near future, with 22 percent willing to pay for training themselves and another 32 percent wishing to share the costs with their employer. This indicates a commitment to professional growth and to the value of training as a means to keep up with emerging trends in the industry. Nearly three-fourths of survey respondents said they still prefer traditional face-to-face training; they hold the same preference for e-learning, either live or self-paced.

For the first time, the study asked about professionals’ preference for “cyber range training,” a multi-disciplinary approach to producing cyber warriors. And while only 41 percent preferred this method of training, more than 80 percent of them found cyber range training to be successful.

What are the hot topics for training?
“In a security discipline that is becoming more inclusive of employees from other departments and externally (for example, with managed security services providers), ramping up communication effectiveness will be essential for the information security professional,” states Michael Suby, Stratecast VP of research at Frost & Sullivan. “Not only will having this skill help in your current position, but it will also benefit the promotion-minded professional who wants to move up in the security ranks.”

“Equally important as the highly technical, hands-on skills is the ability to communicate the value of information security in business terms.”

—David Shearer, executive director, (ISC)²

Adds (ISC)² executive director David Shearer, “Equally important as the highly technical, hands-on skills is the ability to communicate the value of information security in business terms. Developing business proposals and budgets to establish and sustain an information security program is vitally important.”

Shearer adds, “For far too long, information security has been viewed as solely a technical issue, when in fact it is essential to enabling the business. (ISC)² is committed to helping its members develop these essential skills to complement their technical information security abilities.”

Frost & Sullivan conducted the survey for the (ISC)² Foundation, with support from Booz Allen Hamilton, NRI and Cyber 360 Solutions. Visit the Foundation Website at www.ISC2Cares.org to download your copy of the report.
The **projected growth rate** for the information security analyst profession between 2012 and 2020

**SOURCE:** BUREAU OF LABOR STATISTICS, 2014

Do you have what it takes to answer the call?

Elevate your information security career with one of Capella’s new MS in Information Assurance and Security options: **Digital Forensics** | **Network Defense**

*Your future is waiting. Start now.* [CAPELLA.EDU/ISC2 OR 1.866.670.8737](#)
MENG CHOW KANG

Meng Chow Kang was born and raised in Singapore. He is currently director of information security at Cisco Systems and serves as a member of the Cisco Information Security Leadership team. A member of (ISC)²® since 1998, Meng Chow was recently elected to its Board of Directors.

EDITED BY ANNE SAITA

How did you get your first “big break” in information security?

I’m not sure if there was a “big break” per se, but I suppose perseverance and luck played important parts in my development. Having good leaders who were willing to place trust in my potential and to give me opportunities was crucial. That’s also part of luck. In any case, I believe knowledge is part of the preparation for luck, or a so-called “big break,” to strike.

My first diploma was in mechanical engineering. With limited exposure, I signed up for a part-time diploma course in computer studies, when I found an interest in computer systems shortly after I started work in a government office in 1986.

After completing work for the computer studies diploma, I continued with a part-time advanced diploma course in software technology while I worked on a small team developing security software to address some newly found virus problems.

After about five years of part-time studies, I managed to secure a place at Royal Holloway and Bedford New College, University of London, to complete a Master of Science degree in information security. When I returned from the master’s program, I was appointed the head of a security R&D unit. I subsequently moved on to the private sector and continued my career journey in information security as new opportunities to learn and grow came my way.

Have you ever considered another career?

No. It seems that computer security found me, and I very much indulged in it. I have not looked back since getting into this field. I do, however, constantly expose myself to different roles where my knowledge and experience in information security could make a difference. In the process, I also acquire new knowledge and experience.

Asia is a hotbed of IT security activity, isn’t it? What are the biggest information security issues happening in your region right now?

Asian economies are big consumers and importers of IT products and services from those outside of the region, even for economies that have their own IT industry (like Japan, South Korea, and China). As such, the recent spate of data breaches and technology surveillance-related incidents has raised serious concerns over the trustworthiness of technology and related solutions. This raises challenges for both providers and consumers, and perhaps for governments regulating the industry and at the same time needing the technology and solutions to protect critical infrastructure and citizens’ privacy and safety.

Many technology providers are stepping up to meet the trust challenge, by implementing capabilities to provide high-security assurance transparency to demonstrate trustworthiness. Also, various governments are formulating new policies and regulations requiring ever-stringent scrutiny and control over imported technology and solutions. This results in more trade disputes, and narrows the opportunities for more advanced security technologies to be made available and accessible to address the pressing cybercrime issues.

Meng Chow Kang reveals more in our up-coming June 2015 e-newsletter, INSIGHTS.
ADVANCE YOUR BRAND WITH CUSTOM CONTENT

TWIRLING TIGER PRESS IS YOUR PUBLISHING SOLUTION

"...70% of people would rather learn about a company via an article than an ad."
—HARVARD BUSINESS REVIEW

You understand the power of content to tell your value story. And at Twirling Tiger Press, so do we.

We are your one-source publishing solution for great writing and design—keeping your audience engaged through original publications, white papers, blog posts and more.

Let us put our editorial, design and marketing expertise to work for you by creating fresh, contemporary content that expresses your thought leadership.

Contact us today at info@twirlingtigerpress.com.

Twirling Tiger Press Inc. is a custom content and graphic design company that helps you effectively communicate your brand and products.

www.twirlingtigerpress.com

Twirling Tiger Press Inc. is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC)

PUBLICATIONS | WHITE PAPERS | SOCIAL MEDIA
SECURE the power of the cloud

The industry’s new benchmark for advanced cloud security knowledge and competence.

CCSP helps set the highest standard for cloud security expertise, so professionals and organizations can benefit from the power of cloud computing while securing data, applications, and users across the entire IT and information security ecosystem.

**Without strong security, cloud computing will never reach its full potential.**

Reach that potential for you and your organization with CCSP as part of your career roadmap and organizational cloud security strategy.

Learn more at www.isc2.org/ccsp.

Brought to you by (ISC)² and Cloud Security Alliance

© Copyright 2015. (ISC)², Inc. All rights reserved.