TAMING THE CLOCK

STEPS TO HELP YOU GET TIME UNDER CONTROL

Compliance on a Small Budget
Online Dating
Control access. Unleash engagement.

Authentication and Single Sign-On

Improve user experience across apps while protecting against password attacks and data breaches.

Learn more
FEATURES

PROFESSIONAL DEVELOPMENT

14 Taming the Clock
Time management is a perennial resolution for many members who must cram a lot into each day. We offer advice on how to stay in control and get things done. BY DEBORAH JOHNSON

MANAGEMENT

20 Compliance on a Small Budget
SMEs often have the same legal requirements around data security but not the same budgets. An Australian (ISC)² member offers advice on how to meet regulations without breaking the bank. BY DEBI MOFFAT

TECHNOLOGY

24 Love in the Internet Age
One of the most romantic days of the year—in theory, at least—is approaching. Before Valentine’s Day arrives, be sure you and your employees understand the dangers of online dating from a security standpoint, with additional advice on social media by (ISC)² member Ken Novitsky. BY RAJ GOEL
Editor’s Note

TAKING CONTROL OF YOUR LIFE

WHEN I REFLECT on the periods in my life when I felt the most productive, I always return to the nine months I spent earning my graduate degree.

By the time classes started, I had learned to fit a lot into a day as a full-time journalist, military wife and mother and marathoner. Only my running fell into a predicted schedule, but that, too, could quickly be supplanted by breaking news or a sick child. So I scheduled, prioritized, prayed, and consumed a lot of Diet Coke.

It worked.

Despite an unusually heavy class load, four-hour daily commute and time-consuming teaching assistantships, I managed to attain a near-perfect GPA, receive great teaching evaluations, manage a slightly altered family schedule, and even run one of my fastest marathons.

I kept going by convincing myself things would slow down when I graduated, returned to full-time work and switched to half marathons, but of course, a hectic schedule had become the new normal. It took several years, jobs and running injuries before I realized it was time to recalibrate seriously.

That’s why I was excited to read our cover story on time management. I think we all, at some points in our lives, struggle with getting things done while juggling too many demands. This is particularly true for information security professionals, who cannot always control work hours and feel pressure from different stakeholders, all of whom want to be the day’s or hour’s priority.

Whether you vow to gain more control over your time, your relationships, your health, or your finances, I hope this is the year you actually make it happen.

> 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................................................................. 5
Walden University.............................................. 7
(ISC)²................................................................. 13
(ISC)²................................................................. 18
Interop............................................................ 19
Twirling Tiger Press........................................... 23
HIMSS............................................................... 29
(ISC)²................................................................. 31
RSA Conference.............................................. 33
Capella............................................................. 34

© Rob Andrew Photography
From Zero to 60, (ISC)² CyberSecureGov is Advancing the Cybersecurity Workforce.

Join us for an insightful two days as cybersecurity experts from government, industry, and academia share on how to maximize resources in order to keep pace with cyber threats. Attendees will gain an in-depth knowledge on what new threats —and solutions— are emerging, the future legislative and political landscape, funding new initiatives in a post-sequestration reality, effectively adopting federal security initiatives and guidance, how best to recruit, retain, and educate the future cyber workforce, and more.

- Keynotes from leading government cyber security professionals
- Panels with industry leaders
- Three dedicated tracks
- Networking with experts and cyber security professionals
As someone who has been entrusted with information security responsibilities throughout my career, I welcome the opportunity to speak out about the challenges we face on behalf of those working to keep our cyber world safe.

During my past two years as COO here, I’ve seen the organization make positive strides toward establishing a member focus; however, this is a sustained commitment with more work to be done. I want to build on the momentum of our successes while continuing to evaluate areas that we need to improve so that we’re continually striving for excellence in everything we do.

As the new (ISC)² executive director, I want to continue on the path of success we’ve achieved under the leadership of Hord Tipton, whose boundless energy and enthusiasm for all things information security and (ISC)² are unrivaled in the industry. I understand that I have big shoes to fill.

My own background includes 14 years working with the U.S. Coast Guard before moving to the U.S. Department of Interior, where I ultimately served as deputy CIO. At both organizations, I was fortunate to work with some true visionaries who understood the role IT could play in these large, disbursed organizations with diverse missions. The last ten years of my government career, I served at the senior executive level before joining (ISC)² in 2012.

I take my new responsibility of being the leader and public face of this organization very seriously. My first order of business will be to continue to advance our global partnerships to ensure a smooth transition and to continue building rapport with the lifeblood of our organization—the global (ISC)² membership. There’s certainly more work to be done on behalf of the membership to advance our mission globally, and I plan to roll my sleeves up to further that cause.

We have a broad range of initiatives underway, so I will ensure those projects come to fruition. It’s not always about adding new ideas to the pipeline. I’ve always respected people and organizations that demonstrate the ability to make great ideas a reality. During my tenure as executive director, I plan to advance the goals and objectives that our Board of Directors has put forth for the organization.

With 100,000-plus members, some of you will fully embrace the new programs and enhancements coming your way; others may be too busy to participate as much. I hope that at a minimum, you periodically check our website to see what we’re offering that will benefit you in your career.

I look forward to this exciting new challenge of becoming the leader of (ISC)² and hope to meet you at a future event or Chapter meeting.
Answer the Call for Cyber Security Experts With an IT Degree From Walden.

- Doctor of Information Technology (D.I.T.)
- M.S. in Information Technology
- B.S. in Computer Information Systems
- And more

Offering specializations such as Cyber Security, Health Informatics, and Software Engineering, our degree programs can give you the skills you need to join the field.

Get Credit for Your Professional Certifications.

- Certified Information Systems Security Professional (CISSP)®
- ISACA Certified Information Security Manager (CISM)®
- Project Management Professional (PMP)®

Explore our programs at WaldenU.edu/cybersecurity.

NEW REQUIREMENTS FOR CPEs went into effect Jan. 1, 2015, requiring members to submit 40 CPEs annually, compared to the 20 CPEs that were previously required. The new requirement is designed to ensure members stay up-to-date as threats and security solutions continue to evolve.

The required domain-related (Group A) and optional professional development (Group B) CPEs per year for each three-year cycle will now be evenly divided, as shown in the table below. The total number of CPE hours required for each certification remains the same, but they will be distributed equally amongst the three-year cycle. Group B CPEs remain optional and may be substituted by Group A CPEs.

### NEW CPE POLICY

<table>
<thead>
<tr>
<th>CERTIFICATION</th>
<th>TYPE</th>
<th>ANNUAL REQUIREMENT (HOURS)</th>
<th>3-YEAR TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISSP</td>
<td>Group A</td>
<td>30</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Group A or B</td>
<td>10</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td><strong>Total Required</strong></td>
<td><strong>40</strong></td>
<td><strong>120</strong></td>
</tr>
<tr>
<td>CSSLP, CCFP</td>
<td>Group A</td>
<td>20</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Group A or B</td>
<td>10</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td><strong>Total Required</strong></td>
<td><strong>30</strong></td>
<td><strong>90</strong></td>
</tr>
<tr>
<td>SSCP, CAP, HCISPP</td>
<td>Group A</td>
<td>15</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Group A or B</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td><strong>Total Required</strong></td>
<td><strong>20</strong></td>
<td><strong>60</strong></td>
</tr>
<tr>
<td>Associates</td>
<td>Group A</td>
<td>15</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td><strong>Total Required</strong></td>
<td><strong>15</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### SECURITY CONGRESS ’15 NOW SEEKING SPEAKERS

Openings still remain for speakers for the fifth annual (ISC)² Security Congress to be held Sept. 28 through Oct. 1 in Anaheim, Calif., U.S.A.

Once again co-located with the ASIS International 61st Annual Seminar and Exhibits, (ISC)² Security Congress 2015 is expected to bring together more than 20,000 professionals worldwide from both the traditional and information security disciplines.

Congress organizers are currently accepting speaker submissions for these information security tracks:
- Cloud Security
- Swiss Army Knife
- Mobile Devices – Security and Management
- Governance, Regulation & Compliance
- Software Assurance & Application Security
- Malware
- Threats – Management, Detection, Intelligence & Mitigation
- Professional Development
- Forensics
- Healthcare Security
- Women in Security
- Identity/Access Management

To submit a proposal in one of the categories above, please visit https://congress.isc2.org/call-speakers. For inquiries, email congress@isc2.org. (ISC)² will accept submissions until March 2, 2015.
**(ISC)² MEMBER DAVE TYSON NAMED ASIS PRESIDENT**

**DAVE N. TYSON**, CISSP, CCP, has been named the 2015 President of ASIS International.

Tyson is senior director of Global Information Security, Business Process and Technology, for SC Johnson, Inc., based in Racine, Wisconsin, U.S.A. In addition to this position, Tyson also will join the Board Management Committee of the ASIS Board of Directors, which directs the activities between meetings of the full board.

He becomes the 60th president of ASIS.

---

**ONLINE LEARNING COMING TO (ISC)²**

The long-awaited (ISC)² Learning Center will launch in Q2 2015, but (ISC)² members have a chance to see this exciting online learning management system now.

Through (the ISC)² Learning Center, industry professionals will be able to visit the website and easily purchase any of the Live OnLine products, web-based content, and other products available for sale through the portal.

Be sure to check your inbox in coming weeks for more information. To access the (ISC)² Learning Center, visit [https://learning.isc2.org/](https://learning.isc2.org/).

---

Almost one in five children between the ages of 9 and 11 admit to meeting Internet strangers in real life, according to a national survey by the (ISC)² Foundation of 1,214 UK primary school pupils.

The majority (47 percent) of children who arranged a real-world meeting first met the person through online gaming. Next most popular forums were social media and online chats (26 percent).

—From the Nov. 14, 2014 online edition of The Telegraph
NEW (ISC)² BOARD MEMBERS

Thank you to all of the members who participated in elections held in November.

The following four information and software security experts were elected to the 2015 Board of Directors (pictured in order listed below):

- Flemming Faber
  CISSP
  (Denmark)

- Steven Hernandez
  CISSP, CAP, CSSLP, HCISPP, SSCP
  (U.S.A.)

- Dr. Meng-Chow Kang
  CISSP
  (Singapore)

- Allison Miller
  CISSP
  (U.S.A.)

These members join nine other top information security professionals from around the world representing academia, private organizations, and government agencies.

Each of the Board members volunteer to provide strategy, governance and oversight for the organization, grant certifications to qualifying candidates, and enforce adherence to the (ISC)² Code of Ethics.

For a complete list of current Board members, please visit: https://www.isc2.org/board-of-directors.aspx.
GLOBAL SPOTLIGHT: (ISC)² NEW JERSEY CHAPTER

NJ CHAPTER PROMOTES CYBERSECURITY AWARENESS FOR ALL AGES

The New Jersey Chapter of (ISC)², established in May 2012, has made part of its mission to educate every level of the community in cybersecurity. Two projects exemplify this goal.

On October 7, 2014, the New Jersey Chapter co-sponsored and participated in the inaugural New York Metro Joint Cybersecurity Conference (NYMJCSC) held at St. Francis College in Brooklyn, New York, U.S.A., for approximately 350 professionals representing 96 companies and organizations. Aligned with the Department of Homeland Security’s National Cybersecurity Awareness Month, in which the NYMJCSC is a 2014 NCSAM Champion, the program highlighted the latest cybersecurity news and trends and shared practical applications in legal, forensics, audit, and programming for individuals in the information technology/security communities.

NYMJCSC was the first collaborative event of leading information security industry organizations and chapters, including:

• Cloud Security Alliance (New York Metropolitan Chapter)
• InfraGard (New York Metro Chapter)
• ISACA (New York Metro, New Jersey, and Greater Hartford Chapters)
• (ISC)² (New Jersey Chapter)
• ISSA (New York Chapter)
• OWASP (New York Metro Chapter)

Gurdeep Kaur (President), Cindy Cullen (Membership Chair) and Tony Nelson (Treasurer) represented the (ISC)² New Jersey Chapter at the event. In addition to promoting the Chapter’s work, they received sponsorship for their upcoming quarterly Chapter meeting. Kaur described the event as “a solid demonstration of a very successful partnership with other like-minded entities.”

A second community-based project from the (ISC)² New Jersey Chapter was the establishment of a “Junior Chapter” membership category for local high school students interested in volunteering and learning about information security/community outreach efforts.

The first objective the Junior Chapter tackled was the education of senior citizens as to how to safeguard their information and prevent identity theft. The project was led by a 15-year-old high school student who was inspired by an incident that occurred with an elderly member of her family. The student developed a step-by-step prevention guide called “Not in My Name” and presented it at a quarterly Chapter meeting. Several other high school and middle school students have since joined the chapter and are currently working on a “Social Media Etiquette” guide for their peers.

In addition to the Junior Chapter, the New Jersey Chapter also delivers cybersecurity career presentations at high schools and local colleges. They have also established a mentoring group for those looking to get into the profession and actively participate in the (ISC)² Foundation’s Safe and Secure Online program.
ON-TOPIC TRACKING

23 track sessions explored risk engineering, mobile applications, incident prevention and much more, while special features included a challenging quiz for delegates who dared participate and lessons learned from Bletchley Park and Enigma.

THIS YEAR’S (ISC)² SECURITY CONGRESS EMEA INCLUDED INTERACTIVE PANELS, INSTRUCTIVE SESSIONS, AND LOTS OF NETWORKING.

STAY UP TO DATE ON THIS YEAR’S CONFERENCES AT WWW.ISC2.ORG/EVENTS
CSSLP® is the only certification that validates your knowledge and experience in secure software development practices.

Enabling the next generation to

BUILD HACKER RESILIENT SOFTWARE

Get the credential that recognizes your application security expertise. Sign up for our FREE webcast series and find out what you need to know.

education.isc2.org/csslp-webcast
TAMING THE CLOCK

IT SECURITY PROFESSIONALS OFTEN HAVE DAYS WHERE EVERYTHING IS HAPPENING AT ONCE. GETTING TIME UNDER CONTROL IS POSSIBLE WITH SOME PLANNING AND INSIDE KNOWLEDGE

BY DEBORAH JOHNSON

VEN AFTER 20 YEARS in the IT security field, David Doyle continues to face the challenge of the clock.

“It’s the nature of how IT works. It’s constantly evolving and constantly changing, and you have to adjust and adapt on a pretty aggressive level,” says Doyle, director of Information Security and Compliance for Honolulu-based Hawaiian Airlines. “[You have] to be flexible enough to adapt with changing technologies to help support [your customers], but you also have to keep up with the emerging threats and risks.”

“The only reason for time is so that everything doesn’t happen at once.”

—ALBERT EINSTEIN
For IT professionals, that need to “adjust and adapt” challenges the idea of the 40-hour work week. A 2014 survey of 200 U.S. IT executives, conducted by GFI Software of Durham, N.C., U.S.A., revealed that those polled worked an average of 8.5 hours more than their regular schedules. It was much the same in the U.K., where GFI conducted a similar study. There, IT workers put in six hours more than their regular schedules, which is a 48-hour week. As a result, workers in both studies reported missing social and family functions, which added to the stress of the work.

WHERE DID THE TIME GO?

“You can ask me for anything you like, except time.”
—NAPOLEON BONAPARTE

When the day ends, many of us find ourselves wondering what we’ve accomplished.

For a report in the January 2013 issue of McKinsey Quarterly, “Making Time Management the Organization’s Priority,” Frankki Bevins and Aaron DeSmet surveyed 1,500 executives around the world on how they spent their time. Only nine percent said that they were satisfied with how their time was spent.

And in a study of “knowledge workers” in the United States and Europe published in the September 2013 issue of the Harvard Business Review, respondents said they spent an average of 41 percent of their time on “discretionary activities that offer little personal satisfaction and could be handled competently by others.”

Yet despite the dissatisfaction many of us have with how we spend our time at work, tasks are being completed, and goals are being achieved.

“Think about the most accomplished successful people out there,” challenges Laura Vanderkam, consultant and author of 168 Hours: You Have More Time than You Think. “It’s not that they get an extra hour in the day … Whatever they are managing to do with their lives, they are managing to do in the same amount of time as the rest of us.”

The culprit, Vanderkam says, is us. “We tend to spend a lot of time on things that are not as important as we think they are if we asked how much things will matter in a year from now.”

Robert Tanner, management consultant and founder of Business Consulting Solutions LLC, based in Bellevue, Wash., U.S.A., adds that the daily surprises can throw all plans into disarray. “When I coach managers, their approach is less holistic. It’s more execution, more firefighting, more ‘let’s get it done.’”

Put succinctly by Gerry Shukert, IT manager at SeniorQuotes Insurance Services in San Diego, Calif.: “It’s the variables. It’s the unknown.”

TAKING CONTROL OF THE CLOCK

“Time is the scarcest resource, and unless it is managed, nothing else can be managed.”
—PETER DRUCKER (professor, management consultant, author)

While there may be some people who always seem to have their schedules under control, Brian Jaffe, co-author of the IT Manager’s Handbook and vice president of IT Audit at Interpublic Group of Companies (New York, N.Y., U.S.A.), says they might not be what they seem.

“Sometimes it can be a veneer that people are really managing time…but I wonder if that’s just a façade and that inside, they’ve got the same pressure or turmoil, but they just don’t display it,” he says. “They may internalize it and then go home to work until 1 a.m.”

Despite the variables and unknowns, there are strategies and tactics that can give even the busiest IT security professional a bit of control over the remorseless passage of time.

• CREATE A TIME LOG. Want to know where your time goes? Track it, say many experts. Include every meeting, every phone call, every report, even the interruptions. Consultant Tanner suggests approaching tracking your time as you would your finances. “You’d be surprised how those little ATM withdrawals and those trips to Starbucks start to add up. Track every dime. Do the same thing with your time.”

Adds Laura Vanderkam: “Oftentimes what’s happening in an organization is that people are spending time on tasks that aren’t, in fact, the
highest priority task that someone higher up in the chain of command would have identified.”

Once you know where your time is going, you have the information you need to make changes.

• THE PROS AND CONS OF THE DAILY LIST.
There are list-makers, and there are list-haters. Tanner believes that lists can be very helpful but warns that they can also mislead. “Lists are critical, but make sure you assess the list based on importance, not just on deadline.” Vanderkam cautions against too long a list. “Don’t ‘overplan’, because you can’t. You know it won’t go exactly as you planned … Plan a very small number of things that absolutely have to happen, and then the rest of the time is how you optimally respond to things that come in.”

Hawaiian Airlines’ Doyle agrees. “I keep a hit list, or a hot list of the things that are the most pressing, the ones that I have to get to, that cannot be dropped.” And keep it short, he adds. “I like to keep my list really, really small, maybe three to five things that are the must-do’s.”

Interpublic’s Jaffe says that while he’s not a list-maker, he has his own way of keeping track. “I think about it [the day] on the subway on the way to work. If something’s particularly important, I will block out time on my calendar. I’m big on keeping track of emails and putting them into folders.”

• VARIATION ON A LIST. Vanderkam offers another way to organize your time: “Block off the day into different chunks of time. For instance, every morning from nine to noon, I’m going to work off this list of client projects. Then from one to two, I’m going to send out new pitches. Then from two to four, I’m going to do internal meetings.” By assigning major tasks to blocks of time, Vanderkam says, you will (hopefully) get to everything you need to over the course of the week.

When coaching IT professionals on time management, Jaffe recommends providing a time estimate for each project. Start by “chipping away at the small projects first to feel progress,” he recommends. “Then dedicate time to larger, more complicated projects.”

“When I coach managers, their approach is less holistic. It’s more execution, more firefighting, more ‘let’s get it done.’”

—ROBERT TANNER, management consultant and founder, Business Consulting Solutions LLC

• KNOW WHAT’S IMPORTANT. By determining what tasks and projects are crucial to your work, you’ll be better placed to make decisions on prioritization. In coaching professionals, Tanner uses time management guru Stephen Covey’s matrix, as described in Covey’s 1994 book, First Things First.

Tanner advises professionals to look at their work and place their projects and tasks in the appropriate categories. “Quadrants 1 and 2 should be the focus for professionals, with quadrant 1 being the urgent ‘fires’ that need to be put out and quadrant 2 covering the planning, development and training to enhance the company’s priorities.” Then, he adds, anything that is falling into the remaining quadrants is not important. Re-assign some of those tasks and beware of the time-wast-
ers, he counsels.

What is also important to IT security professionals, says David Doyle, is to remember “that we are here to enable the business—remaining aware that we are here to support the business.” And to understand better what that support looks like, Doyle encourages those on the IT side to “step outside of what we do…and start meeting with the different layers of the business…and understand what’s important to them.”

OUR OWN WORST ENEMY

“Lost time is never found again.”
—BENJAMIN FRANKLIN

Most of us have the time to do what we need to do, says Vanderkam, but we need to review what’s important to us and what isn’t. She adds that often, we try to do too much and don’t “recalibrate” during the day.

“One of the reasons people wind up working extra hours or staying late is because time gets away from them during the afternoon.” She encourages professionals to make a late afternoon check-in. “An hour before quitting time, or when you intend to get out the door, you perform a triage assess: what absolutely has to get done and what does not. Because you are going to be at work the next day, and a lot of this stuff can wait.”

Another way we can defeat ourselves, warns Jaffe, is by failing to see both our abilities and our environment clearly. “For a lot of us, we are overly optimistic or not accounting for other problems that can crop up.”

The lack of communication is another danger, warns Doyle. “There’s that one group that is really hesitant to ask for help. Keeping that communication line open is really important.”

Stress over conflicting priorities will eat up time as well. When faced with that kind of overload, Tanner suggests asking yourself this question first: What is the absolute worst thing that will happen if I don’t do this? When people start there, it helps them prioritize.

The crises that arise can cause havoc with daily needs and plans. Making sure you have the time and ability to deal with a crisis when it arises can be challenging, says SeniorQuote’s Shukert: “Being able to put out fires is crucial, but then you need to solve the problem to prevent it from happening again. That’s about finding the right partners and the right processes and evaluating the actual needs.”

ONE METHOD DOES NOT FIT ALL

“Time is really the only capital that any human being has and the only thing he can’t afford to lose.”
—THOMAS EDISON

Time management is often an individual challenge: trying to find your way back to your priorities, hoping you can shave off some time on one thing to make time for another. That idea of “saving time” in bits and pieces is misguided, according to Vanderkam.
“There are all sorts of things you’d like to do to save a few minutes on, here and there, but time doesn’t work that way. When there is something you really want to do, you make the time for it. Instead of looking to save time here and there, find things you really want to do that are so urgent and compelling to you that you let everything else sit.”

Sorting through the tasks and crises of the day may require intervention.

Managers should step in when necessary, says Hawaiian Airlines’ Doyle. “The onus is really on us to help make sure we’re identifying those instances that people are having problems with time management.” And, he notes, not everyone works the same way.

“There are some people who just like to sit down and plug through a queue…they don’t want to be fighting fires. There are other people—they thrive on that sort of chaotic crisis type of scenario. Part of it is understanding your people.”

Jaffe agrees and notes that “people think differently. Don’t look at disorganized people as second-class citizens. Just because someone doesn’t manage their time the same way I do doesn’t mean their way is bad or not as good as mine.”

For most of us, the 40-hour work week is a relic of the last century (and maybe even earlier than that). Making the best use of our time, at work and at home, requires effort, a little discipline, and perhaps some guidance.

After all, as the late Steve Jobs of Apple, Inc. once observed, “It’s really clear that the most precious resource we all have is time.”

DEBORAH JOHNSON is managing editor of InfoSecurity Professional magazine.
INTEROP
Las Vegas  APRIL 27 – MAY 1, 2015
EXPO: APRIL 28 – 30
MANDALAY BAY CONVENTION CENTER, LAS VEGAS

Connecting the IT Community

IT Pros come to Interop to see the future of technology, the outlook for IT, and the possibilities of what it means to be in IT.

In 2015, Interop Las Vegas features three unique conference programs to serve the needs of the entire IT team.

Critical Education for IT Management and Staff

InformationWeek Conference
An Exclusive Program for CIOs and Technology Leadership

Cloud Connect
Empowering the Cloud-Enabled Enterprise

GET A FREE EXPO PASS WITH CODE: PAISC2
www.interop.com/lasvegas
THE AUSTRALIAN YOUTH cancer support organization CanTeen faced a situation common to many smaller organizations. CanTeen National Projects Advisor Deepika Ratnaike was involved in ensuring the organization pass a compliance audit of their new online platform while in the midst of building the actual platform.

“As a charity, we didn’t have a lot of resources to throw at either project. We also needed a lot of technical knowledge to understand the requirements and recommendations,” Ratnaike explains.

SMEs typically have less access to technical skills, so they need to be a bit creative when faced with a compliance challenge.

An effective compliance program can protect an organization from myriad of potential problems that could lead to financial collapse, even criminal penalties. Large corporate entities can fund significant staff to develop, monitor and maintain compliance, but small-to-medium enterprises (SMEs) have far fewer resources to apply to compliance. And as new regulations are introduced and existing ones are tightened up, achieving and maintaining compliance is becoming a greater challenge for smaller organizations.

There are ways that small organizations—with miniscule budgets to match—can benefit from the knowledge and skills of larger organizations and achieve compliance without breaking the bank.
1. **Own Your Compliance Plan**

A common mistake smaller organizations typically make is to treat a compliance audit as something that happens to them, rather than a process that they need to manage proactively. The most successful compliance programs are those that are managed like a project. They involve resource planning, task prioritization, deadlines and effective communication. The organization should make all the parties involved aware of their roles in the project and communicate to them how they can best support the project. For this to work well, senior management support is imperative, and appointing a project manager can be helpful.

2. **The Sooner, the Better**

The earlier a change is made in a project, the cheaper it is to make.

Engage security advisers in the early stages of the project rather than waiting until the end to perform a compliance audit and then hitting them with a long list of non-compliances to resolve. By getting the right advice in the requirements-gathering and design stages, SMEs can design and build a solution that is compliant - resulting in a much smoother (and less stressful!) audit process. This represents a cost savings, as the amount spent on consulting fees up front can more than be offset by avoiding non-compliance repairs later in the project.

Ratnaike goes on to describe CanTeen's integration of compliance and platform development:

“We found it useful to complete the security audit early in the project, as it allowed us to incorporate security recommendations as we were building the platform. We also sought advice from security consultants, which enabled us to implement preventative practices, rather than having to react after an incident occurred.”

3. **Look Outside Your Organization**

When developing a compliance program from the ground up, don’t assume you need to hire new staff or up-skill your existing employees. It may be more cost-effective to obtain the expertise you need externally. For example, if you don’t have a suitably skilled IT administrator, you might elect to ask your hosting provider to perform security monitoring tasks. Build relationships with specialists in areas where your internal skills are lacking. This way, you only pay for their skills when you need them.

Another cost-effective alternative for SMEs comes through the emergence of policy generators and subscription services. Simon Litchfield, co-founder of PrivacyPolicy.com.au, has teamed up with a lawyer to develop one such service.

“Many smaller organizations have fairly straightforward data usage requirements and don’t need to spend a lot of money on specialists to write a privacy policy for them,” he says. “Instead, they can use a policy service and get a privacy policy that is updated in line with changes to the law.”

Of course, it is important to review the output from these services before taking them on board, as responsibility for it ultimately lies with your organization.

4. **Keep It Simple**

While larger organizations have the opportunity to develop their suite of documentation over time, SMEs often don’t have much in the way of internal documentation and may not have any policy-writing skills available in-house. And, many assume (and fear) that these documents need to be massive, detailed tomes.

On the contrary, a procedure doesn’t need to be lengthy to be of value. In fact, the opposite is often true. The purpose of the documentation procedure is to record step-by-step instructions in a way that is easy to understand and follow. It may be that a bulleted list will suffice.

Simple procedures are:

- Quicker to write
- Easier to maintain
- Easier to train your staff on, and
- Easier to follow

5. **Less is Best**

Minimize the data you hold to reduce your compliance overheads.

**Delete the data you no longer need.** This applies to all organizations but is particularly relevant for those on a tight budget. If you don’t need to keep a piece of information, then don’t!
Retaining information has costs associated with it, such as:

- Ensuring you protect the data appropriately and in line with any applicable legislation
- Keeping the data accurate and up to date
- Storing the data
- Backing up the data

The more information you have, the higher the cost. So, perform regular audits to identify what information you have, determine whether you need it, and, if not, get rid of it (in a secure manner, of course).

Avoid collecting sensitive data whenever possible. Sensitive data is particularly costly to keep in a compliant manner, due to the extra requirements for protecting it. The less you collect, the better. Analyze all of your data collection channels and ask the question, “Do I really need this information?” Chances are, you’re collecting more than you need to—perhaps for historical reasons that no longer apply. Update your data collection processes regularly, and keep them as lean as possible.

Reduce the handling of sensitive data. The fewer people and systems that come into contact with sensitive data, the smaller your compliance hit will be. For example, if you are obliged to encrypt a piece of data and that data resides in five separate software systems, that’s five different encryption problems to solve (and that’s not even taking backups into account)! If you can reduce the number of systems the data resides in, you can make a tangible reduction to the amount of work required to encrypt it.

6. Something for Nothing

Take advantage of the many free tools available.

Consider freemium/freeware. Sometimes also referred to as “crippleware,” these are different takes on the same concept. Basically, you get a “light” version of a software product for free. It may be missing some features that you can get from the premium offering, or it may have limits in place (for example, a maximum number of users, or reduced data usage), but you can get some very useful tools this way. This is especially ideal for SMEs who have reduced staff and data.

Utilize open source software. Similarly, there are many security-oriented open source offerings available now, such as Intrusion Detection Systems (IDS) and encryption products. The catch with these tools is that you need someone with the skills to install, configure and manage the product on an ongoing basis, and if a bug or security flaw is detected in the product, there will be no one around with the skills to fix it in a timely manner.

To combat this, Ryan Schipper, senior security consultant at Redcore, advises, “Many companies are now offering paid services and support for existing open source products. This means small companies can save on ongoing licensing costs but aren’t up the creek if something goes wrong.”

Purchase second-hand equipment. You can buy almost anything second-hand these days: servers, firewalls, SSL accelerators—the list goes on. As long as you perform a clean install, or reset factory defaults, second-hand equipment can provide a good, cheap alternative for those with limited financial resources.

Nicholas John, also from Redcore, says, “I’ve heard of one company that bought an HSM [hardware security module] second-hand off Ebay.”

You obviously don’t get the same level of assurance you would with an HSM whose history you know, and you would have to choose its application wisely, but it provides an option for cash-strapped organizations.

7. Avoid Point Solutions

Schipper advises SMEs to seek out products and services that can satisfy multiple compliance requirements at once instead of buying point solutions. “Large companies can apply economies of scale, while SMEs generally cannot.” Many security product vendors now offer bundled product suites, and it’s worth doing your research to see what is available.

In isolation, the techniques described here aren’t monumental, but together, they provide an SME with substantial savings and efficiencies on its journey toward compliance.

DEBI MOFFAT, CISSP, is a Sydney, Australia-based security consultant with a passion for helping organizations improve their security.
YOU'RE UNIQUE. YOUR MESSAGE SHOULD BE TOO.

\ CONNECT \ 
Fresh, contemporary white papers and publications that express your thought leadership

\ ENGAGE \ 
Outstanding editorial, design and marketing draws in your target audiences

\ INFORM \ 
Great storytelling and visual content puts you ahead of competitors

WORDS + DESIGN
Twirling Tiger Press Inc. is a custom content and graphic design company that helps you effectively communicate your brand, products and services. We offer white papers, publications and more. Contact us today at info@twirlingtigerpress.com.

©Twirling Tiger Press Inc. is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC)
EVERAL YEARS AGO, New York photographer Nev Shulman fell in love with a woman named Megan, whom he met on Facebook. Over time, he began to wonder if Megan was perhaps being less than truthful, and, with a film crew, went to Michigan to track her down.

Instead of meeting the love of his life, Shulman came to realize he’d been having a relationship with a married woman named Angela, who had created Megan’s profile.
Shulman documented the tale in a U.S. movie called Catfish and parlayed the film’s popularity into a cable television series of the same name. In each episode, someone begins to suspect they are being duped by an online boyfriend or girlfriend they have never met in person. In most cases, their suspicions are confirmed by the end of the show.

Most of us shake our heads at people’s gullibility, but in fact, it’s all too easy to fall victim, especially if we are actively looking for a meaningful relationship through the Internet. Whether it’s match.com, eHarmony.com, okcupid.com, christianmingle.com, jdate.com for Jewish singles or shaadi.com for Indian families (or the hundreds of Chinese, Russian, and other regional and language-specific sites), there is an online community willing to play matchmaker.

But lonely hearts aren’t the only ones on those sites. Predators, psychopaths, criminals, and even employers are lurking there, too, potentially taking advantage of what these sites and apps promise to deliver: potential companionship. But along with this promise comes a host of privacy and security threats. Most of us in IT security are well aware of the risks when dating online. Are your coworkers?

Private Isn’t So Private
The real problem with most dating sites is the amount of information people post about themselves in order to find a suitable match. The questionnaires are legendary for their length and depth. And the responses create a profile that never goes away.

Some people, after creating a profile, end up in a relationship, but, more commonly, they abandon the site after a while and maybe delete the app. But do they remember to delete their profile completely? Those who don’t likely do so partly from ignorance and partly from convenience in case they want to get back in the game and avoid the onerous process of filling in all those fields again. So, their profile is still alive and well and available to anyone who knows how to access it.

People who use the “let’s-meet-up” app, Tinder or Snapchat, a photo delivery app which promises that pictures will disappear on command from the recipient’s cell phone, aren’t any safer.

- In January 2014, 4.6 million Snapchat users had their data dumped on the Internet. As reported in the January 3, 2014 edition of Forbes.com, the data included usernames and partial phone numbers.
- In October 2014, a third-party app called Snapchat was breached, and the often sexual photos of many Snapchat users were leaked. Pcmag.com reported on October 13, 2014 that nearly 200,000 photos had been leaked.
- A breach on the mobile dating app Tinder lasted approximately two weeks and leaked full name, date of birth and location, despite the app CEO’s assertion that the breach was of a much shorter duration, as reported in the July 25, 2013 edition of qz.com.

So, how does all this pose security threats to the enterprise?

Online Dating – Toxic to the Workplace
Consider a corporate executive with a secret life. Professionally, she can be tracked through her LinkedIn profile (which may be managed by her marketing department) and her bio on the company’s Website.

But what about her private online life, which includes profiles and photos on several dating sites? Anyone can easily put the public and private online personas together.

Most of the dating sites/apps expose her current physical location, marital status, sexual or dating preferences, things she likes to do for fun, and the type of person she likes to do them with. This executive is likely to be a little more candid if she believes all of this information is safe from public view. And, she believes that lying to protect her identity defeats the purpose of finding someone with the same interests.

But the confluence of the two could impact her career, now and in the future. Employers have been known to reject job candidates based on finding and reading their profiles on dating sites. A 2012 market study by Eurocom Worldwide and reported in the April 2013 edition of Forbes.com revealed that one in five technology executives said that they had not hired a candidate because of what they saw in the candidate’s social media profiles.

CONTINUED ON PAGE 28
IT HAPPENS. And it happens more often than you think. A comment on a friend’s Facebook or hyperlink in a blog post lures you to click, and once you do, you instantly regret it. This isn’t remorse for what’s written—or left unsaid—but for being duped into downloading malware, like “malvertising” that appears to buy traffic from legitimate ad providers in order to place malicious ads on popular YouTube videos. Before you know it, your machine’s become part of a massive botnet. And it only gets worse, once your personal information is harvested and your online identity is used to find new victims.

There is nothing new about social engineering being used as part of clandestine information reconnaissance for an illegitimate purpose. But despite decades of warnings, malware still proliferates. And for several years now, social media has been the conduit of choice.

Giving Away Too Much
While most of us are wary of emails from foreign princes needing to park some royal money, we aren’t as suspicious when a request with a hyperlink comes from someone we know (or would like to know).

Yes, social media is a good place for the bad guys to leverage social engineering techniques to continue their attack. The more you expose yourself and your personally identifiable information to the world, the more susceptible you are to being used as a lure.

Typical information people share about themselves through social networks includes:

- Name and photo
- General location where they live, hang out and travel
- Employer and job title
- Professional skills and connections
- Prior employers
- Education, including schools and graduation years
- Personal interests/hobbies

And in some cases, we involuntarily share information such as a user’s IP address; host name; and URL history.

Know the Scams
All this information is a boon to those seeking to exploit it for nefarious purposes. It can be used to select targets and/or to create custom-tailored enticements or just plain, good old fashioned exploitation. A 2014 Symantec Intelligence Report listed the top five attacks or exploits that can use this information:

Fake Offers. These scams invite social network users to join a fake event or group, offering incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number. This is the most common kind of attack, accounting for 52 percent of exploits.

Manual Sharing Scams. These use the victims to do all the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends. This is second most common type of exploitation (37 percent).

Likejacking. Using fake “Like” buttons, attackers trick users into installing malware and may post updates on a user’s newsfeed, spreading the attack. This type of exploitation occurred 8.5 percent of the time.

Fake Apps. These are applications provided by attackers that appear to be legitimate but carry a malicious payload. The attackers often take legitimate apps, bundle malware with them, and then re-release them as a free version of the app. This accounts for 1.7 percent of exploitations.

Comment Jacking. Similar to likejacking, this type of scam relies on users clicking links that are added to comments by attackers. The links may lead to malware or survey scams. As an exploit, it’s still uncommon, accounting for less than 1 percent of attacks.

Setting up a fake account and building trust with owners of valid accounts is also a way to spread malware. What better
way to gain confidence than to pretend
to be someone with whom your target audience would love to connect? And the more people connected with the legitimate account, the better the odds of exploitation.

Another type of scam involves exploiting such trust but does not necessarily involve malware scenarios per se. For example, a common investment scam using social media, called a “Pump-and-Dump,” is used to manipulate markets. “Pump-and-Dump” schemes involve trumpeting a company’s stock (typically small companies) through false and misleading statements to the marketplace. These false claims could be made on social media, as well as on bulletin boards and chat rooms. Once these fraudsters “dump” their shares and stop hyping the stock, the price typically falls, and investors lose their money.

**Take Control**

So what can be done, especially given most of us want to build an online presence to improve our careers, maybe even our offline social lives?

First and foremost, keep up with software patches, especially those fixing vulnerabilities in Web browsers.

Additionally, here are some suggestions from Microsoft’s Safety and Security Center:

**Be linkophobic!** Fear of links is good. Clicking on links can lead to bad things. This is probably the most common way that malware gets spread. No matter who sent it to you or where it is, use caution when clicking on it.

**Be careful about what you post about yourself.**

This may give someone potential insight into how to social engineer any security question you may have set up to prevent unauthorized access to your account. Along this line, it may be wise to set up “false” answers that only you would know to such security questions to thwart this kind of hacking.

**Don’t trust and try to verify.** This is a little different spin on the old proverb about trusting no one, even your mother, but it’s just as valid when it comes to receiving email messages. That email you just received from your mom may very well be a malicious actor who has just hacked her account. Call Mom first to see if she really sent it, especially if it contains links.

Watch out for fake login pages. Clicking on links (in a phishing or bogus email) that appear to take you to a legitimate site login may very well bring you to a fake page that can capture your credentials. For example, a link showing “www.yourbank.com” may really take you to “www.captureyourpassword.com.”

**Don’t accept just anybody’s connection.** If you don’t know the person or even if you do, make sure the account they are using is a real one. The days of trying to appear popular by “friending” as many people and connections as you can are over. It turns out that, just like real life, it’s all about quality over quantity.

**Read privacy policies, especially when there’s a change.** Do not assume your content remains private if there are changes that reset accounts to more public modes. Is it fair? No, but it’s your job to stay on top of privacy policy changes.

**Remember—anything you post can be permanent.**

There is no telling where that information will turn up in the future, even though you thought you deleted it and it was long gone.

**Practice safe hex!** Be careful about installing that add-on when you can’t be sure who wrote it and if it will do what it says it will do.

**Avoid using social network sites at work.** You might be opening a door, allowing your network to be infected. You also may be violating your employer’s Acceptable Internet Use Policy.

Perhaps this year, one of your personal goals is to become more social, or maybe it’s to become less social and to focus on other pursuits besides updating your Facebook or Twitter accounts hourly or daily. Regardless of where you see yourself online in 2015, be smart about what and how you share and connect.

KEN NOVITSKY, CISSP, is an IT consultant for a major northeast utility. His work focuses on IT security issues, as well as IT internal controls.
The Tricks of the Cyber Villains

This is not to suggest everyone who uses social media or dating sites is going to fall prey to scams or interlopers. We know from all of the success stories touted on television and radio, and perhaps among your networks of friends, that isn’t the case. Dating sites have become an acceptable means of matchmaking in today’s society.

However, it’s important for everyone in your organization (and, quite honestly, extended families and friends) to be aware of the threats “honey traps” (attractive male or female spies to trap a victim into gaining access they otherwise might never obtain) pose to them and their organization.

Penetration testers and criminals routinely create LinkedIn profiles of attractive female recruiters to conduct reconnaissance on their targets, as documented on techday.com. Sometimes they fabricate the information in a profile; other times it’s lifted from other members’ profiles. Some companies even post fake profiles to lure people into paying monthly fees for non-existent dates. In November, 2014, the U.S. Federal Trade Commission (FTC) fined JDI Dating, a U.K.-based online dating site, for fabricating profiles and charging a fee to connect. On November 1, 2014 c/net.com reported that JDI was ordered to pay $616,165 for posting fake profiles.

Divorce, Cyber Style

Social media can also wreak havoc on your personal life. Match.com likes to tell you in their commercials that one in five marriages and relationships begin online. What they don’t tell you is that in the U.S., according to a 2010 study by the American Association of Matrimonial Lawyers and reported in The Guardian on March 8, 2011, four out of five divorces begin with information found online. And in the U.K., according to Divorce-Online, one out of every three divorces cites Facebook as the cause for divorce.

More and more matrimonial attorneys are now requiring that their clients given them their Facebook, Twitter, and Gmail account credentials as part of the divorce process. In the July 19, 2013 edition of Family Lawyer Magazine, the authors advise their readers on how to mine their clients’ (and their opponents’) social media data to protect their clients (and find damaging data on the opposition).

How to Avoid Online Heartbreak—and Worse

That’s the rub. And that’s why so many people provide so much sensitive, private, valuable data—data that’s also easily available to a penetration tester, social engineer, criminal, stalker, or opposing counsel.

Valentine’s Day is approaching, and many of your colleagues (perhaps even you) will decide it’s time to join a dating site. I strongly recommend that you educate yourself and your users about the long-term dangers of these sites.

A few tips:

- Ask them to keep track of which sites and apps they use. In a few weeks, remind them to delete accounts/profiles of sites they’re no longer using.
- Keep an eye on your Web traffic for new, interesting or suspicious dating websites and apps.
- Remind your users to avoid installing unapproved/unauthorized apps on their corporate phones and tablets.
- With approval from management and legal, use data from social media and dating sites as case studies in your security awareness training.
- For parents of teens and tweens, have a conversation with them about emotional, reputational and legal dangers of social media, including sexting and Snapchatting.

Consider this a friendly reminder that the Internet has democratized crime, lowered the costs for conducting espionage and data theft, and made our jobs working in information security much, much more challenging.

As security luminary Dan Geer once said, “In the world of network computers, every sociopath is your neighbor.”

RAJ GOEL, CISSP, is a New York-based cyber civil rights advocate, author, and speaker. He is the owner of Brainlink International.
Access a vital tool in your journey to health transformation at HIMSS15: the power of information. Discover answers to pressing questions, explore market-ready solutions, hear expert perspectives on critical issues, and network with thousands of like-minded health IT professionals, clinicians and executives from around the globe.

Join (ISC)^2 at and harness the power of health IT at HIMSS15. (ISC)^2 members receive a discounted rate, CLICK HERE for details.

Register now: www.himssconference.org
WE WANT TO start the new year with a big tip of the hat and pat on the back to the many members whose generosity made 2014 one of the (ISC)² Foundation’s most successful years yet.

Three hundred new members volunteered as part of the (ISC)² Foundation’s worldwide initiative, **Safe and Secure Online**, bringing top cybersecurity experts into classrooms and community centers throughout the year. Since the program began, more than 1,200 (ISC)² member volunteers have helped nearly 150,000 children learn how to protect themselves online and become responsible digital citizens. This is done through volunteer training and compelling materials that empower the next generation of Internet users to take charge of their own online safety and reputations.

The Safe and Secure Online program was most prominent on Safer Internet Day in February, 2014, when member volunteers presented safety tips to nearly 10,000 children in a single day. This year’s SID is Feb. 10. It’s a great time to get involved in the program.

Due to your donations, we were able to launch Safe and Secure Online in Ireland last year. Those volunteers now join colleagues in Canada, Hong Kong, Switzerland, the United Kingdom, and the United States. Based on requests in 2014, more than two dozen countries hope to join them; however, we first must collect more donations to help fund them.

Last year, the (ISC)² Foundation joined efforts with the U.S. Department of Homeland Security’s (DHS) **Stop.Think.Connect.™** campaign. The campaign’s overarching goal is to help Americans of all ages understand the risks that come with using the Internet and encourage them to take steps to protect themselves online. This effort is a partnership comprised of federal and state governments, industry, and non-profit organizations, all sharing resources and working toward a common goal. You should first see results of this partnership during Data Privacy Day on Jan. 28 and this October’s Cybersecurity Awareness Month.

In the spring of this year, the (ISC)² Foundation is excited to unveil the results of our sixth **Global Information Security Workforce Study** (GISWS). The study has...
become a well-respected industry benchmark referenced by governments, employers, professionals, and industry stakeholders around the world for more than a decade.

Each year, the (ISC)² Foundation reevaluates its popular Scholarship Program for additional opportunities. Among this year’s improvements will be changes in application schedules.

- Faculty Exam Voucher applicants now have four application periods to seek opportunities to become certified, thus further certifying these cybersecurity experts’ experience and credentials in the field.
- The (ISC)² Foundation Women’s Scholarship program will accept applications now through March 31, 2015.
- Undergraduate and graduate application periods will open March 1 and run through June 17.

This staggered application period allows those who applied for the Women’s Scholarship to be recommended for consideration for a Graduate or Undergraduate Scholarship if they don’t receive one in the Women’s category.

The new schedule also provides graduate and undergraduate applicants with additional time to submit their final spring semester grades.

All of our 2014 accomplishments and goals for this year couldn’t happen without the support we receive from you, the (ISC)² members who help to continuously improve information security through awareness programs and educational opportunities. Thank you, and we look forward to working with you—and for you—in the coming 12 months.

(ISC)² Program Enhances Cybersecurity Education throughout the Global Academic Community

(ISC)² invites you to explore the Global Academic Program (GAP). Through the GAP, (ISC)² collaborates with an ever expanding network of university members to establish a joint framework for delivering essential skills to support the growth of a qualified information security workforce. Industry-Academic cooperation can bridge the workforce gap between the large demand for qualified cybersecurity professionals and the amount of skilled professionals who are prepared for the market.

(ISC)²’s Global Academic Program areas of focus:

EDUCATION. Integrating the importance of education, certification and continual learning (CPEs), thereby increasing workplace value.

RESEARCH. Thought leadership collaboration via roundtables, executive panels and workforce analysis.

OUTREACH. Connecting with future IT professionals thru the Global Chapters, Young Professionals Network and Foundation.

For further information check out the Global Academic Program (ISC)² website at: www.isc2.org/academic. Institutions looking for more information on the Global Academic Program should contact Dr. Jo Portillo at academic@isc2.org.
5

Minutes With...

JAVVAD MALIK

Javvad Malik is a London-based senior analyst within the enterprise security practice 451 Research. He’s also among the most active (ISC)² members, serving as a presenter and the EMEA representative on the magazine’s Editorial Advisory Board. EDITED BY ANNE SAITA

Q

How did you become involved in information security? And who was your first mentor?

During my degree (business information systems), I had the opportunity to take my third year out to work in the industry. I happened to land a job in the IT security department of a bank. That was during a time that nobody really knew what IT security was, but I ended up really enjoying my time there.

As for my first mentor, I actually spent most of my early career without one. This is something I really regret, because once I did find my first mentor, my career and personal development grew by leaps and bounds. My first mentor wasn’t your typical mentor; he was actually a colleague of mine, Jitender Arora. He was one of the first people who truly believed in me and instilled that self-belief in me too. I attribute a lot of my success today to his support and guidance, without which I’d probably still be in a job I don’t enjoy.

What do you consider the biggest security or privacy issues in EMEA at the moment and during the next year?

In my opinion, the biggest issues are that the goal posts are continually moving. New legislation comes up that is often ill-thought out or a knee-jerk reaction to something else. We have things like the ‘cookie law,’ which is wholly inadequate, despite good intentions. More recently, we’ve had the case whereby Microsoft is coerced by courts to hand over data held outside of the U.S., on non-U.S. users. There’s also the ongoing debate as to the adequacy of safe harbor. Up against an ever-changing backdrop, it’s nearly impossible for companies and individuals to plan their security or privacy strategies for the long term.

Within five years, what do you think will be the top five skills every infosecurity professional will need to be promoted?

Being promoted within infosecurity shouldn’t really be much different from being promoted in other disciplines—high level execs need the same broad set of skills, such as:

• Leadership – including the ability to share power
• Change management – the ability to adapt quickly
• Being outcome-focused – if you’re not delivering results, you’re not valuable
• Seeing the big picture. How many security professionals understand the company from the perspective of the CEO?
• Great communication and interpersonal skills.

Javvad Malik reveals more in our upcoming February 2015 e-newsletter, INSIGHTS.
Register now for RSA® Conference 2015

The theme for this year—CHANGE—is a timely reminder of the importance of challenging today’s security thinking. Attend RSA Conference to keep up with the changing dynamics of cyber security.

- **23 tracks**—including 3 new ones!
- **350+ Sessions**
- **400+ Exhibitors**

Experience these exciting programs:
- RSAC Innovation Sandbox
- Live streaming video on RSAC TV
- Great lineup of **Keynote speakers**
- (2) Official (ISC)² CBK® Training Previews
  for CSSLP® and CISSP-ISSMP® credentials

Register Now! [www.rsaconference.com/isc2](http://www.rsaconference.com/isc2)

FOLLOW US ON: #RSAC
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