Mobile device malware takes social engineering to a new level with human vulnerability.
What if you could:

• Have your SIEM up and running in **less than 15 minutes**?
• Easily configure your Security Management Solution **yourself** – without the help of hired consultants?
• View the overall strength of security and state of compliance in a **single pane view**?
• Discover and mitigate security threats **before** they impact your core business?
• **Demonstrate compliance easily** with just a few simple mouse clicks?

You can! NetIQ security management solutions will get you there.

Join NetIQ for a **FREE WEBCAST SERIES** focused on the anatomy of modern security threats and how to build a strong defense in your organization. You will learn simple but valuable techniques on how to get your security solution up and running in minutes instead of days. You will gain invaluable knowledge on how to detect and mitigate security threats and learn about the best tools on the market to help you accomplish these goals while demonstrating compliance to current regulations.
features

10 The Human Factor of Social Engineering
Mobile device malware takes social engineering to a new level with human vulnerability.
BY CRYSTAL BEDELL

14 Are You Ready for Next-Gen Security Audits?
New technologies, various social networking architectures and compliance regulations are a recipe for next-generation security auditing.
BY PETER FRETTY

18 How to Self Promote the Right Way
Advance in your career with strategic self-promotion.
BY SANDRA GITTLEN

also inside

3 (ISC)² Makes a Strong Push
Executive Letter From the desk of (ISC)²’s Executive Director Hord Tipton.

4 Moderator’s Corner
Views and Reviews Highlights from (ISC)²’s event moderator, Brandon Dunlap.

6 FYI
Member News Read up on what (ISC)² members worldwide and the organization are doing.

20 Shelter from the Economic Storm
(ISC)² Foundation Results from The Foundation’s 2012 Career Impact Survey.

21 Chapter Passport
Join a local (ISC)² Chapter and make a (secure) difference in your community.

22 Confronting Mobility and the Cloud
Q&A (ISC)² board member Dan Houser discusses mobility and cloud security.

24 A New Authentication Paradigm
Global Insight Bringing an old technology back to life.
BY LARS MAGNUSSEN
Malware Data From Over 600 Million Systems Worldwide

The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from internet services and over 600 million systems worldwide to help you protect your organization, software, and people.

View the Security Intelligence Report at www.microsoft.com/SIR
Safe and Secure for all Generations

THE (ISC)² MISSION: SERVE NOT ONLY INFOSEC PROFESSIONALS, BUT ALSO REACH OUT TO THE NEXT-GENERATION.

IT SEEMS A NEW YEAR has just begun, and suddenly, we’re nearly three months into it. We’ve hit the ground running, with new Board members, a new career survey (see page 20) and new plans for the 2012 Security Congress conference in September. And we’re not slowing down anytime soon. We have much to look forward to this year, thanks to our ever-energetic, dedicated staff and members.

As I look at how far we’ve come in our 20+ years, I can’t help but remark on how our organization and our membership have evolved. We originally focused on CISSP as the credential for someone who mastered security and required five years for that certification. We have since broadened our mission to serve other communities, developed other robust credentials, and we continue to add to our list of certifications and resources.

Our approach today is to reach out to all generations, to develop an awareness of and an interest in information security as a stable yet vibrant career choice. Our member volunteers now have more than 1,000 hours in teaching our Safe and Secure Online program, and we’re working with other non-profits in educational segments around the world to help spread the knowledge throughout secondary schools to make cyber security awareness a lifelong pursuit.

We know that security threats are at the top of your radar. It’s our job to arm you with the most useful and informative resources in order to prepare for—and combat—the most difficult security issues. The top challenges of note fall into three areas:

Social media: This communication channel is becoming a way of life, blurring the boundaries between our personal and professional realms. From businesses, to educational institutions to young children, social media is a vehicle that facilitates not only global communication but also social engineering and identity theft.

Mobile technology: Mobile technology is much more sophisticated than ever. As Jayson E. Street, CIO at Stratagem 1 Solutions, notes in our “Human Factor of Social Engineering” article in this issue (see page 10), mobile phones are not phones. They are “computers that make phone calls.” Mobility alone changes the security landscape.

Application security: Social media, mobile technology and applications create the perfect security storm. The more applications on the network, the more vulnerabilities in databases and elsewhere. We are continually monitoring these areas so we can provide you the professional development tools you need to stay ahead of them.

If you have expertise in any of these areas, we’d love to have your input—and your presentations. As we prepare for the second annual Security Congress, which takes place in September in Philadelphia Penn., U.S.A., we are seeking your knowledge to share with other members and conference attendees. You can submit your papers online at https://www.isc2.org/conferences.aspx.

In the meantime, be sure to check out this issue’s articles on social engineering, audits, and, of course, the Foundation column, which features results of the (ISC)² 2012 Career Impact Survey.

Sincerely,

W. Hord Tipton
CISSP-ISSEP, CAP, CISA, CNSS
Executive Director, (ISC)²
2012: The End of the Beginning?

According to some ancient calendars, 2012 marks the end of days for life on Earth. As the so-called fateful year begins, I can’t help but think they had it all wrong. This year is like every other; a new year with a new beginning. Perhaps it’s my optimism as I emerge from the long dark winter. Maybe I haven’t lost my youthful idealism (naïveté?) after all. Either way, I think that this is our time, as security professionals, to push through our historical baggage and seek a new way forward.

This year should be the year that we break out of our IT silos and run through the organization with our banners held high above our heads. We should be seeking to co-opt or coerce our peers across the org chart to come to our side. This is the year of convergence, but not in the way that we have been led to believe.

2012 is the year we push our business sense in the right direction. Metrics, as we will discuss in this issue of InfoSecurity Professional, are a big part of our business mindset. While we have spent a lot of time in the past couple of years discussing the metrics of security, I pose the following question: Is there really such a thing as a metric for how secure we are? Instead, I suggest we track our operations like they were a business unto themselves. I would go so far as to posit that there is no such thing as a security metric, only performance metrics about how well our security program is functioning.

To that end, we can develop our metrics programs with an eye toward other areas of the enterprise in which we can become much more ingrained. For example, as (ISC)² has continued to deliver their Security Leadership Series on the software development lifecycle, we have begun to introduce more topics in our Web series. In the waning days of 2011, we discussed the risks associated with open-source software (link to the archive, which qualifies for CPEs, can be found here: http://bit.ly/OpenSourceRisks). This represents some phenomenal opportunities to introduce quality-oriented security metrics into our development processes. This is but one example of how we can wave our banner across the enterprise, showing ways in which the security function can help fix areas of inefficiency and quality, with a keen eye on the business benefits of oversight.

Continuing in the same vein, and while it may seem like a long way off, (ISC)² and ASIS will be joining forces again in September for Security Congress, this time in Philadelphia, Pa., U.S.A. Based on last year’s success, this program promises to truly bridge the gap across the great divide between traditional and logical security.

I’m feeling pretty good about 2012. What about you?

As always, I look forward to continuing the conversation,

Brandon Dunlap
Managing Director of Research, Brightfly
bsdunlap@brightfly.com
www.brightfly.com
Are you considering the next steps to further develop your information security knowledge and progress your career? Take it to the next level with a CISSP Concentration. CISSPs with two years of professional experience in one of the functional areas of architecture, engineering or management may seek a CISSP Concentration.

Watch the FREE webcasts on each domain and the value of holding the CISSP-ISSAP, CISSP-ISSEP or CISSP-ISSMP to learn more. Concentrating may open up new opportunities, including more demanding roles in larger enterprises, more education opportunities and a specialized certification to recognize your talents.

Watch the Free Domain Webcasts for the CISSP®-ISSAP®, CISSP-ISSEP® or CISSP-ISSMP®
www.isc2.org/previews
New Year, New Board

(ISC)² is proud to announce the following new members of its Board of Directors, who will serve three-year terms, effective January 1, 2012. The (ISC)² Board provides governance and oversight for the organization, grants certifications to qualifying candidates and enforces adherence to the (ISC)² Code of Ethics. Please welcome the following new board members:

- Daniel D. Houser, CISSP-ISSAP, CSSLP, Senior Security and Identity Architect for a Global 100 healthcare organization (U.S.)
- Wim Remes, CISSP, Manager of Information Security at Ernst & Young ITRA FSO (Belgium)
- Prof. Jill Slay (AM), Ph.D., Fellow of (ISC)², CISSP, Dean: Research in the Division of IT, Engineering and the Environment at the University of South Australia and Professor of Forensic Computing (Australia)
- Greg Thompson, CISSP, Vice President and Deputy CISO at Scotiabank (Canada)

The elected board officers for 2012, serving a one-year term include:

- (ISC)² Board Chair, Freddy Tan, CISSP (Singapore)
- (ISC)² Vice Chair, Benjamin Gaddy, CISSP, CSSLP, SSCP (U.S.A.)
- (ISC)² Board Treasurer, Flemming Faber, CISSP (Denmark)
- (ISC)² Board Secretary, Richard Nealon, CISSP, SSCP (Ireland)

Introducing: (ISC)² Security Central

(ISC)² Security Central is the new online resource for security professionals and the public at large. It focuses on providing valuable resources for those interested in the security field and increasing security awareness. (ISC)² Security Central brings together information from (ISC)², industry organizations, security practitioners and more. In addition to searching the site for useful resources, (ISC)² members and other security professionals are encouraged to contribute their security events, publications, white papers, podcasts and more to share with other site users. Stay tuned for more details soon on how you can contribute your resources to the site and begin using (ISC)² Security Central.
(ISC)² and ASIS International Team Up Again

2012 (ISC)² Security Congress Registration Now Open

(ISC)² AND ASIS INTERNATIONAL have teamed up once again for the largest security event of its kind in the world. The second annual (ISC)² Security Congress (www.isc2.org/conferences.aspx), colocated with the ASIS International 2012 58th Annual Seminar and Exhibits, will take place September 10-13, 2012 in Philadelphia, Pennsylvania, at the Philadelphia Convention Center. These events will bring together more than 20,000 security professionals from all disciplines, providing attendees with professional development opportunities that span both the traditional and information security landscapes.

(ISC)² members have exclusive access to members-only events such as a networking reception and Town Hall Meeting, not to mention a significant discount on regular conference registration pricing. To register, visit www.isc2.org/congress2012

SAFETY FIRST: Safer Internet Day

SAFER INTERNET DAY, organized by Insafe, which is co-founded by the European Union, is celebrated annually in over 65 countries throughout Europe in early February. The Day recognizes the importance of the Internet in the lives of children. Now in its ninth year, the theme for 2012’s Safer Internet Day, connecting generations and educating each other, emphasized the complexity of challenges currently faced by children in their digitally connected lives. On February 7, 2012, (ISC)²’s UK-based Safe and Secure Online volunteers visited 19 schools, educating more than 4,000 students across the UK. For more on Safer Internet Day, visit www.saferinternet.org/web/guest/safer-internet-day.

Stay tuned for more details soon on how you can contribute your resources to the site and begin using (ISC)² Security Central.
Survey Says: Positive InfoSec Career Outlook for 2012

A SPECIAL THANK YOU to the 2,250+ (ISC)² members around the world who participated in the 2012 (ISC)² Career Impact Survey. The results are in, and the infosec industry remains steadfast with a bright future ahead. Read the Foundation column on page 18 for more information. Full results are available at https://www.isc2.org/industry-resources.aspx.

NEW! Introducing…

THE (ISC)² KNOWLEDGEVAULT interactive video series offers quick advice and features from (ISC)² and InfoSecurity Professional magazine. It's a one-stop shop for security resources that can also be shared via Twitter, Facebook, LinkedIn, etc.

Take a look at this online video and content series, and check back often for new videos, valuable security resources and exclusive online issues of InfoSecurity Professional magazine!


Tout It Out!

See the latest blog posts by fellow (ISC)² members on the (ISC)² blog at http://blog.isc2.org. Share your innermost thoughts, advice and expertise with other industry pros today.

(ISC)² Helps Aspiring Pros Prepare for Careers in Cyber Security

(ISC)² HAS ADDED the Certified Secure Software Lifecycle Professional (CSSLP®) and Certified Authorization Professional (CAP®) credentials to its Associate of (ISC)² program to help fill the pipeline of qualified information security professionals. Candidates who pass the CISSP®, CSSLP, CAP or SSCP® certification exam but lack the professional experience required to become certified will be granted Associate of (ISC)² status until they meet the necessary experience requirements (within the allotted timeframe for their preferred certification). The Associate of (ISC)² program is also a great resource for universities around the world looking to assist graduates as they transition into the professional world.

As Seen in SC Magazine

THE SC MAGAZINE COVER STORY, The New Wave; Modern Security Education, examines hands-on programs for students pursuing Infosec careers. The (ISC)² Foundation’s scholarship program is highlighted in this article.
(ISC)² Global Awards Program
People, processes and policies are all necessary to protect and secure information assets. (ISC)² recognizes the professionals who are leading the way and making a difference in this ever evolving industry, honoring their tireless efforts and standards of excellence in the field of information security.

For more information on the awards program, gala dinner ceremony or to nominate an outstanding information security professional, visit awards.isc2.org.
Attackers are conducting social engineering attacks via smartphones and tablet PCs to gather personal data from unsuspecting users. When those same devices are used to access the corporate network and its resources, the corporation is at risk. “There’s a significant chance that whatever credentials are stored on the phone will be collected, and a large chance that those credentials are shared by other apps within the corporation,” says Ryan O’Horo, senior security consultant at IOActive.

With these credentials, attackers can log into the VPN and get access to the corporate network, read users’ sent emails, write and send email, access employee portals and collect contact information to conduct further social engineering attacks.

“There are plenty of reports on mobile malware and its pending explosion. It seems as if the media and antivirus vendors would have IT professionals holding their breath as they wait for a wave of malware to hit smart phones and tablet PCs. While the threat of mobile malware is real and likely to become more serious, another critical threat to mobile devices is already well underway. It doesn’t rely on vulnerabilities in the operating system, so it can’t be patched. It relies on human vulnerability. We’re talking about social engineering.

Social Engineering on Mobile Devices
Social engineering attacks can be carried out in a number of ways on a mobile device. Similar to spam and phishing attacks via desktop IM and email clients, attackers are using SMS messages and mobile email to social engineer users of mobile devices. SMS message spam can become a nuisance...
and rack up exorbitant service fees for the user. Forged emails and email spam can appear more legitimate on a mobile device, given the screen real estate and users’ propensity for brevity when sending email from a mobile device.

Attackers also use social engineering to "sell" illegitimate applications to users. Social engineering techniques are used to convince the user to download applications. The app may be promoted as solving a particular problem or be associated with a popular movie or other cultural trend to make it look appealing. Simply offering the application free of charge motivates unsuspecting users to click the download button. Often times, the actual application may serve a legitimate purpose, but collect personal data in the background when the user accepts the terms and conditions for use.

Research firm Loudhouse conducted a mobile device security survey for vendor AdaptiveMobile and found that an average of 84 percent of all apps downloaded were free, compared to just 16 percent paid. Furthermore, users are willing to risk their personal information to avoid paying for applications. Twenty-five percent of survey respondents said they would be willing to download a free app that might contain personal information over a paid app that definitely did not.

Loudhouse evaluated the data usage of 40 applications drawn from the top 20 free applications and top 20 free games available for download across the iPhone and Android stores and marketplaces. Case in point: from those 40 applications, Loudhouse found that collected data was passed on to more than 146 domains.

Psychological Principles at Work

Social engineering attacks via mobile devices work on the same principles as those delivered via desktops. "The topic is new: the considerations for social engineering related to mobile platforms. But they’re not much different from our classic social engineering threats that are still persistent, and we’re not dealing with it very well," says O’Horo.

Jason Rhykerd, consultant, SystemExperts Corp., agrees. "It’s the same concept and the same philosophy, just a new attack vector," he says.

Regardless of the attack vector, social engineering exploits a user’s propensity to trust others. The attacker takes advantage of this trust to manipulate the user into performing an action—say, clicking on a link in an email, or sharing confidential information. The difference between a social engineering attack delivered via a desktop vs. a mobile device, from a psychological perspective, is "the threshold of acceptability," says Jayson E. Street, CIO of Stratagem 1 Solutions. "The threshold of caution is lower. People are less cautious on their mobile device than on a computer. They are more likely to click on a link," Street says.

Street explains that the same email sent to a recipient on a mobile device and a recipient on a desktop is more likely to be opened by the mobile device user. Users have been educated on social engineering threats for computers, but they don’t yet understand that those threats also exist on their mobile devices. "We’ve schooled ourselves that there are threats for computers; be careful about email on your computer. Information security has not figured out a proper way to explain to people that it’s not a phone; it’s a computer that makes phone calls," says Street.
The trust that users have in their landlines has carried over to smartphones. In the eyes of the user, the device is a phone, not a computer. This is evidenced by the buying cycle, explains Street. People don’t buy a new computer every year. And yet, this is becoming the norm for smartphones. Meanwhile, smartphones are becoming increasingly accessible to users who are less tech-savvy. As the price goes down, the number of users goes up. Attackers can easily exploit the inherent trust people have in their phones and use it against them.

The form factor and way that mobile devices are used also lend themselves to a lower threshold of acceptability. For example, it is easier to forge an email to be read on a mobile device because users are likely to write sparingly. A user writing an email on a mobile device is likely to be on the move, perhaps in a rush. The email gets right to the point. Because of the small keyboard, recipients are more forgiving of grammatical and spelling errors.

Users are also more likely to click on a link delivered to them on a mobile device than they are to click on that same link via their desktop. “People want to do as little as possible to get what they want,” says O’Horo. That means clicking on the link without taking any precautionary measures, especially when those precautionary measures are difficult to execute.

“We’ve trained people to hover over a link to see where it’s going or to type directly into a browser instead of clicking. But these things are harder if not impossible on a cell phone. Users would rather click on a link than type it, and hovering over the link is not easy to do on a phone,” says Rhykerd.

**Defense Measures**

Defense measures are in order to protect end-users and corporate assets. “It goes back to the basics. One of the most important factors with social engineering, phishing and spam is education and understanding. We don’t click on links unless we know what they are. It’s a simple answer. But it’s an honest and true answer as well,” says Rhykerd.

Corporations can have policies about what can be on mobile devices, but it doesn’t mean they have the tech controls as well. That’s where the human element enters the picture. “With social engineering, the weakest link is the human, and it’s always different. The most bang for your buck is that end-user education. With different attack vectors creeping up on us, it’s time for some updated education,” Rhykerd says.

User education starts with teaching people that their smartphones and tablet PCs are mini-computers that require cautionary measures similar to their desktops and laptops. However, users do not patch their mobile devices and for some vulnerabilities, no patches exist. For example, Street says Apple does not release patches for iOS, so every single user still using older iPhones remains vulnerable. There are apps to help secure Android smartphones, but those are less vetted and may cause more harm than good. For this reason, users need to be more careful with their mobile devices than they currently are with their desktops.

“When we’re talking about social engineering, the patch is called awareness. It’s called education. People are smart and intelligent. They just need to be made aware. They aren’t going to do something to expose themselves, they just need to understand what the threat is and that it’s real,” Street says. (SC)

Crystal Bedell is a Washington-based, award-winning writer specializing in information security and computer networking.

---

**Become an IEEE Certified Biometrics Professional®**

**Why CBP?**

The IEEE Certified Biometrics Professional® (CBP) program has two major components: Certification and Training. Professionals and organizations can both benefit from the IEEE CBP program.

Key advantages are:

- Prove your knowledge
- Increase your credibility
- Learn a baseline of industry knowledge
- Train employees
- Gain a competitive advantage

Learn more and register today! [www.IEEEBiometricsCertification.org](http://www.IEEEBiometricsCertification.org)
NEW TECHNOLOGIES, VARIOUS SOCIAL NETWORKING ARCHITECTURES AND COMPLIANCE REGULATIONS ARE A RECIPE FOR NEXT-GENERATION SECURITY AUDITING. by Peter Fretty
And as change occurs at superfast speeds, enterprises rely heavily upon new technologies and processes to provide true competitive advantages. For security professionals, this means it’s time to prepare for the next-generation security audit.

The next-generation security concept encompasses everything from multi-barrier network protection to context-aware computing to artificial intelligence, explains Damon Petraglia, CRISC, director of forensic and information security services with New York City-based Chartstone Consulting.

“When you combine new and advanced technologies with social networking, different architecture approaches, cloud computing and confusing compliance regulations, you have the recipe for a thousand different approaches to information security and security auditing,” he says. “Each of these—social networking, architectures, cloud, and regulations—must be considered on many levels including business need, return on investment as well as a risk management framework. The question is simply: If we implement a given business solution, can the risk to the organization be reduced to an acceptable level while retaining maximum benefit of the solution?”

According to Petraglia, the difficulty addressing this question is that far too often the audit mentality drives security professionals. “This may be effective for compliance purposes, but compliance does not always equal security,” he says. “Security professionals need to understand that compliance is yes or no, on or off, black or white, and security is a million shades of grey. No system is ever 100 percent secure, and the security professional must understand that any given business needs to function within an acceptable level of risk. It is this balance that the organization must strive for and the security professional to assist or guide in implementing.”

Michael A. Davis, CEO of Tinley Park, Ill., U.S.A.-based Savid Technologies, Inc. agrees, adding that these new technologies and business models change the auditing paradigm because they require auditing on third parties at deeper levels.

“The problem with these factors is that most of the other disruptive technologies auditors had to deal with were simply new technologies—new, faster and better ways to do something everyone understood,” Davis says. “However, social media and cloud computing are new business models and methods of collaboration, meaning many audits need to start by simply understanding the factors before trying to audit them. Also, most IT audits deal exclusively with IT. Whereas cloud and social media incorporate non-IT folks—meaning the auditors’ communication skills must improve as well.”

Organizations can prepare themselves for success by revising and improving their security risk management process to have the ability to address special topics outside the normal annual assessment, explains Doug Landoll, Denver, Colo., U.S.A.-based author of The Security Risk Assessment Handbook. “They can also ensure assessment professionals are aware of the risk associated with new technologies, threats, and regulations,” he says. Davis suggests hiring outside help to assist if your assessors are not familiar with these new technologies.

There is also a need for security professionals to focus on improving their understanding of the business processes, security and technical perspectives, as well as risk management. “Security professionals need to be much more diverse and dynamic now than ever before. They need to understand the business’ industry, standards, and applicable requirements, and the core and advanced security concepts called upon,” says Petraglia.

Petraglia adds that the real key is being able to integrate all of these aspects so the security professional can holistically view the posture of a given network rather than by individual security compliance requirements. “The security professional must be able to understand the interdependencies and interactions between platforms and technologies, and identify inherent weaknesses and vulnerabilities as a result of the interdependencies—all while providing technical and procedural solutions to ensure maximum business process with minimum level of risk,” he says.
WHY NEXT-GEN SECURITY AUDITS?

Here are a few of the key components fueling the need for next-generation security audit procedures:

**SOCIAL NETWORKING:** Whether through company-sponsored blogs, employee access to Facebook, or outsiders posting negative Yelp reviews, an organization needs to first understand its exposure through a social media risk assessment, explains Doug Landoll, author of The Security Risk Assessment Handbook. “These risks can be remediated through improved security awareness training, updated policies and procedures, and the implementation of new technology or services,” he says.

**CLOUD COMPUTING:** In this scenario, services and business unit systems are handled by an external service instead of an internal IT department. To be prepared for the next-gen audit, security professionals need to understand how the cloud provider plans to meet organization security requirements, and demonstrate that they will continue to meet them as they evolve,” Landoll says. “A cloud service risk assessment can document the security requirements, point out the areas of risk, and provide recommendations for required contractual elements necessary to maintain adequate security.”

**COMPLIANCE REGULATIONS:** Compliance regulations change often, and their interpretations and accepted application even more so. As such, keeping up with PCI v2.0, HIPAA/HITECH/ Meaningful Use, and the constantly changing privacy regulations can be an insurmountable task. “Organizations need to change their approach from chasing regulations to proactively creating a security program based on addressing risks,” says Landoll. “Such a program typically already contains the essential elements called for in regulations.”

FIELDING FRESH PERSPECTIVE

Organizations need to understand and employ the basics first, then the advances in technology or next generation, explains Petraglia. “Anything can be transitioned into the business processes with little or no difficulty. Both the business and security professional need to realize that technologies such as cloud or social media are increasingly necessary for the viability of the organization; it is simply how to minimize the risk when implementing the solution,” he says. “Any business or technical process has a lifecycle. It’s crucial to incorporate core security concepts and controls into the lifecycle of any given process.”

According to Petraglia, taking a basics-first approach will ensure better security as well as better control of the investment as security is not retrofitted. Security must be considered from conception through disposal of technical and business process by both the organization and the security professional. “Next-generation technologies and concepts are easier to deal with from either a business or security perspective if one understands the basic concept of risk management,” he says. “Integration and advanced technology is here to stay and will continue to evolve at speeds faster than we’ve ever seen. Unfortunately, the same can be said for the threats that face our businesses, systems, and data. Managing and balancing the risks through the thorough understanding of the technologies, security, and business processes by both the business owners as well as the security professionals is the key.”

A REFINED APPROACH TO SECURITY

For many, the concept of working with increasingly third-party data sources—such as social media and the cloud providers—means the perimeter of the organization starts to melt away, and organizations need to embrace a refined approach to security. This is a significant transition according to Davis.

“Most security professionals use security policies that follow the castle and moat paradigm, where the company has a bunch of data on a bunch of servers at its internal data center. In this scenario, the company controls what goes in and out by putting guardians at the front gates and forcing people to come in over a moat,” he says. “Firewalls, intrusion detection and prevention systems, and Web application firewalls all work following this paradigm, but every major breach analysis has shown that data is much less likely to be stolen because of a vulnerability in the transport mechanism.”

However, it’s important to realize that the biggest risk is not on the outside. It often involves the people who live and work within the castle—authorized and authenticated users with legitimate access to data, whose network access can be taken over by malware and attackers, explains Davis.

“Cloud services, globalization, and collaboration have turned the security paradigm on its head as legitimate users are using these services to get work done, but don’t realize the security implications,” Davis says. “The most effective way a security professional can adapt to the new environment is to implement data-centric security. To do that, we need to articulate what makes data-centric security different from what most security professionals are doing now.”

The data-centric approach works whether dealing with social media, cloud, or the next big technology advancement, Davis says. He suggests referring to the ‘Four W’s’ for the data-centric security model: Where is the data? What is the data? Who has access to it? And why do they need access? After all, Davis says, no matter what the technology does in the future, your data is still data, and it needs protection. (5C)

Peter Fretty is a freelance business and technology journalist based in Michigan.
Gain crucial cyber security skills for your senior level career

With our prestigious MSc in Information Security by distance learning you will:

- Gain expertise in the technical, legal, commercial and people aspects of Cyber Security.

- Tap into the commercially relevant knowledge of Royal Holloway’s leading academics, which is based on their research and practical consultancy experience.

- Earn CPE credits on standalone modules.

Join our professional network

You will become part of a network of over 2,000 industry professionals who have participated in Royal Holloway’s cyber security programmes.

‘This course has the best reputation. I would thoroughly recommend it.’

Andy Smith has over 20 years experience in information security. He chose Royal Holloway as he was looking for a Masters programme that would provide the theoretical underpinnings to support his practical experience.

Find out more
www.londoninternational.ac.uk/infosec

Join Royal Holloway on facebook and contribute to the debates on information security: www.facebook.com/ISGofficial
How to Self Promote the Right Way

Self-promotion doesn’t have to be a dirty word. A good strategy can help you advance your career.

by SANDRA GITTLEN

Like most careers, to rise up the ranks in security, you have to be a self-promoter; sharing your wins with your supervisors and the company as a whole. Yet typically, calling attention to oneself runs counter to the “keep a low profile” credo adopted by most security professionals.

“There’s an inherent secrecy in security that keeps people from tooting their own horn,” says Seth Levenson, an executive career coach for the technology, scientific and financial industries in Brookline, Mass., U.S.A. “They also tend to think their accomplishments should speak for themselves.”

Unfortunately, these headstrong beliefs keep many in IT security stuck in a rut.

To contend for leadership positions, security professionals must fundamentally change. “They shouldn’t get turned off by the term ‘self-promotion,’ which has a pejorative meaning. Instead, they should consider sharing accomplishments an essential part of career advancement,” he says.

A significant obstacle for many security professionals is morphing from an introverted expert in studying alert and event logs to an extrovert who contributes to the business as a whole. The higher up you go in the organization, the less time you spend actually doing the job, and more time is spent communicating to others how the job is done, according to Levenson.

Expecting someone to change overnight is a recipe for disaster, according to Joanne Kossuth, CIO of the Franklin W. Olin College of Engineering in Needham, Mass., U.S.A. Kossuth, who oversees security as part of her executive role, says some security professionals need to be coached in business skills early on so that the transition is easier for them.

For instance, a lower-level security person tends to overwhelm their supervisors with too many technical details. As they climb the corporate ladder, they learn to parse what’s relevant for their audience. “Running into my office and saying that ‘Port X is pushing too much Y’ doesn’t cut it. I need to know why it’s important and how you’re going to resolve it,” Kossuth says.

Here are some tips on how to progress from being the person following security strategy to the one setting it.
Dos and don’ts for self-promotion

**DO**  Scope out realistic advancement opportunities within your organization.

**DON’T**  Threaten that you’ll quit if you don’t get promoted.

**DO**  Share the positive impact you’ve had by highlighting initiatives you’ve led or participated in across the company and their results.

**DON’T**  Blanketly state that you’ve single-handedly effected change.

**DO**  Seek out educational or training opportunities.

**DON’T**  Attend so many events in a row that your daily duties can’t be covered and the budget is drained for co-workers.

**DO**  Work with your manager to achieve your goals.

**DON’T**  Seek help from his or her supervisor without his or her knowledge.

---

**Start at the Start**

Security professionals who are ready to advance their career should look closely at an organizational chart and figure out a reasonable path.

For instance, do you want to stay on the technical side of things or start to focus more on business as a whole? Are you willing to manage people?

The answers to these questions will illuminate gaps in your hard and soft skills. For instance, if you want to move into the business side, then you might want to take college or continuing education courses in finance, marketing and other key areas. If you lack management experience, then you can attend workshops to gain basic skills. And if you want to broaden your knowledge of the organization’s core values, then you can sign up for brown-bag lunches about each division or ask business unit leaders to help you get up to speed.

**Communicate Your Intent to Your Manager**

While it might seem daunting, sharing your career goals is a critical step in achieving them. Going behind your supervisor’s back is often a poor strategy that can backfire. “Most supervisors want to help and have access to necessary resources,” Kossuth says.

Managers can gain budget approval to send you to professional development seminars and other educational opportunities. They also have insight into the current state of business and the organization as a whole that could impact your career path.

Before you ask for the big meeting with your boss, make sure you have a sensible plan, says Beth Ross, an executive career transition coach in New York, U.S.A. For instance, if traveling to a multi-day conference is on your list, figure out how your job will be covered during that time.

Managers must understand why your professional growth would be advantageous to the company, she adds. She recommends creating a list of five bullet points that specify the contributions you’ll make to the company initially with training and certification and, ultimately, a higher position.

**Develop a Fan Base Beyond Your Cubicle**

With such a heads-down position, security professionals often find themselves at a loss when it comes to gathering a cheering committee.

Doing simple things, such as taking the long way to the lunchroom, can quickly alter this reality. You’ll have the opportunity to say hello to co-workers and eventually strike up longer conversations that help you better understand their job functions, Levenson says.

You also can join corporate-wide committees to encounter employees in other business units. However, you must actively participate in the meetings to be seen as a team player, Ross warns.

Security professionals can get noticed without stepping too far out of their comfort zones in some cases, according to Kossuth. She recommends volunteering to develop and lead training sessions on usage policies and procedures. Or you can offer to do weekly email blasts to the organization on timely topics such as viruses and fraud. These tasks also establish you as a knowledge leader who can carefully communicate risks and resolutions—a highly regarded skill among the upper ranks.

**Prove You Have Skin in the Game**

To be considered for a promotion, you have to be seen as invested in the overall well-being of the company.

One approach would be to translate everything you learn at seminars, workshops and the like into an opportunity for the company. For instance, if you learned about a specific product that would make workers more efficient or add to the bottom line, explain why in a brief memo. Share handouts or brochures with peers, managers and executives, Ross says.

She encourages security professionals, as they get more exposure to other business units, to identify ways to improve processes or save money.

Security professionals should take time to listen to and advise peers without expecting immediate personal gain. Be careful not to be seen as an opportunist or shameless self-promoter.

**Do Your Job Well**

A surefire way to get ahead in a company is simply to do your job well. If you’re busy trying to get to the next level and unwittingly open up the company to risk, you won’t get very far.

Work with your manager to set a reasonable schedule that ensures your core work will get done while you fill out your portfolio.

Getting ahead should never mean falling behind in your day-to-day responsibilities. (65C)

---

Gittlen is a freelance business and technology writer in the greater Boston area.
Infosec Careers: Shelter from the Storm

DESPITE A WAVERING ECONOMY, INFORMATION SECURITY CAREERS OFFER STABILITY AND UPWARD MOBILITY.

ALTHOUGH THE ECONOMIC STORM continues to cast a dark cloud around the globe, the information security profession offers professionals shelter from the storm. That’s just one of the telling highlights for infosec professionals uncovered in a new career management research study of (ISC)² members conducted by the (ISC)² Foundation.

The Foundation’s 2012 (ISC)² Career Impact Survey shows that nearly all of the 2,258 professionals who responded were employed in 2011. Of the few unemployed, half were without a job for some portion of 2011 of their own volition, either to pursue professional development, to relocate geographically, or to retire. Other findings include:

- 96% of respondents are currently employed.
- Of those unemployed during 2011, 2% were laid off, and 2% were unemployed of their own volition.
- Of those who sought employment last year, most relied on job websites, social media and networking for job seeking.

Advancement and salary opportunities drove 35% of professionals surveyed to seek new cyber security positions in 2011. And those who stayed in their position also saw increases in compensation. Of the 35% who changed jobs last year, 53% did so because they had advancement opportunities. And, nearly 70% received salary increases last year, while 55% expect to receive increases in 2012.

New jobs are being created daily in the information security industry, and there is a bright outlook for job creation and greater budget flexibility in 2012 as well.

- Roughly 34% of respondents experienced a new-hire increase last year, although 27% saw an increase in layoffs.
- Around 30% of survey respondents expect information security budgets, equipment purchases and new hires to increase in 2012.
- 51% of respondents plan to hire information security staff over the next year.

The information security industry remains focused on the security risks presented by mobile devices (personal or business) and cloud computing. Of those surveyed, 56% reported increased security risk in 2011, with 38% attributing most of that activity to mobile devices. Focus on specific skills when hiring:

- 81% of respondents said an understanding of information security concepts is an important factor in their hiring decisions. Other top factors are directly related experience (72%) and technical skills (76%).
- Top skills hiring managers seek are: operations security (55%); security management practices (52%); access control systems/methodology (51%); security architecture/models (50%); risk management (49%); telecom/network security (45%); applications/system development security (44%); and cloud/virtualization (35%).

Ensuring there is a steady stream of qualified, certified information security professionals to protect society from digital threats remains an issue. About 80% of respondents indicate that they are having a difficult time finding people with the right skills and aptitude to fill vacancies. To ameliorate this problem, (ISC)² members can post their resumes for free on Career Tools, which employers can search for free. (ISC)² also periodically hosts career assistance programs, such as the career fair that will be held at the 2012 (ISC)² Security Congress.

At the (ISC)² Foundation, we’re using the Safe and Secure Online youth education program to introduce youngsters to the profession. What can you do? Consider donating to the Foundation in support of youth education and scholarship programs. Volunteer to go to local high schools to discuss your career with students, and encourage them to enter this exciting, interesting, and secure field.

To see the full survey results, visit https://www.isc2.org/industry-resources.aspx. (ISC)²

—Julie Peeler, Director, (ISC)² Foundation
(ISC)² Chapter Membership: The Value Proposition

SINCE THE LAUNCH of the (ISC)² Chapter Program in September 2011, we have received more than 70 petitions to form chapters around the world. (ISC)² members are eager to network with other local professionals to share knowledge, discuss current industry trends, exchange resources and help educate the community about information security.

Through (ISC)² chapters, members can spread awareness of the profession and educate the public on the dangers of cyber security threats, especially among school-aged children, as well as teachers and parents through the (ISC)² Safe and Secure Online program. It provides a valuable opportunity for chapter members to use their skills to help secure their local communities.

Why are members interested in joining an (ISC)² Chapter, especially when there are many other chapter organizations from which to choose? Here are some of the responses we received from (ISC)² chartering chapter members:

- "Belong to a local forum for networking with local professionals;"
- "Stay up-to-date on new technologies and current trends;"
- "Promote the value of (ISC)² certifications among employers and professionals;"
- "Create awareness and growth of the information security profession;"
- "Contribute knowledge and resources to fellow colleagues;"
- "Educate non-security professionals about protecting their information assets;"
- "Develop leadership and presentation skills;"
- "Reinforce the status of (ISC)² credential holders in remote locations of the world;"

The main purpose of the (ISC)² Chapter Program is to serve the needs of our members. By joining a chapter, (ISC)² members belong to a local network of like-minded professionals who are working toward a common goal. For those members who are not satisfied with the security organization that in which they are currently involved, being a member of an (ISC)² Chapter provides them the opportunity to contribute or make a difference elsewhere.

This is the time for you to make a difference—for your community and for yourself. Don’t wait. Get involved today.

(ISC)² Chapter Directory

Check out the new, interactive map on the (ISC)² Chapter Directory. It now distinguishes chartering chapters from those that are already established. Find an (ISC)² Chapter near you by visiting: www.isc2.org/ch-directory.

If a chapter doesn’t exist in your area, consider starting one. Visit www.isc2.org/ch-start for details (member log-in required).

—Jayda Shriver, Chapter Program Manager
Embracing the Cloud Evolution

DAN Houser, an (ISC)² board member for the past three years, is a senior security and identity architect for a global healthcare organization. He leads a team of security architects who provide security and identity strategies, roadmaps, secure models, and reference architectures.

Q: You’ve worked as an information security professional for various industries, such as banking, healthcare, and education. What stands out as the common security aspect of all three industries?

While the risk tolerance between industries differs, the fundamental issues are all the same: how do we enable the business to meet its objectives with limited capital, and at the right risk model, while protecting vital intellectual property? All businesses struggle with managing a burgeoning identity architecture, and their architecture teams are always adapting to a stunning rate of change. Those patterns are largely the same across industries. As security professionals, we are trying to figure out what cloud means to our business, and many of us are both cloud service providers and consumers of cloud services. All of us are dealing with consumerization and what it means when 80% of your users are bringing their own smartphones and tablets to work.

Process change is another common issue. IT security vendors are usually selling tools, not processes. As my CTO at a bank said, "A fool with a tool is still a fool"—that is, adding a tool to a problem where you have ignorance doesn’t resolve the ignorance. I think that’s universally true. You have to address personnel, process, and technology, and process change is always harder than tool change.

Q: On which new healthcare security initiatives are you currently working?

Cloud and mobile. My company is working aggressively on exploring the business case for cloud-based models for our service. We already offer several as innovative cloud solutions, and those bring unique security challenges because it’s changing...
我们的业务模式在某些情况下。我们在第二个成功“自带设备”计划中，该计划已经取得了正确的风险和可使用平衡。我们也在部署移动解决方案来为我们的客户立即提供信息访问，以改善整体患者护理。这是一个非常令人兴奋的时间，领导安全倡议在医疗保健！云安全，无论哪个行业，仍然是不确定的。

Q: **What are the biggest security issues, and how do you see them changing?**

我认为，大多数云模型是我们已经使用了十年的。唯一的例外是基础设施即服务（IaaS），这是一个最近的创新，但已被有效地用于过去的网格和分布式模型。

我认为，云服务实际上是虚拟化和服务导向架构的演变，而不仅仅是革命。安全问题并不一定与我们之前看到的实现模式不同。这仅仅是以云实现的速度发生了巨大变化。

身份仍然是扩展安全云存在的重要因素，以及数据安全、应用程序安全，并且必须解决和管理第三方信任关系。

Q: **Where do you see the biggest security challenges in the next few years?**

我认为，我们在未来几年面临的最大问题将是数据被推到边缘，消费者化驱动着巨大的创新和变化。我们已经看到了临界点，消费者正在购买比公司更多的计算机。这不仅对IT，而且对一直基于 perimeter security的原有安全模型是一个巨大的变化。

身份是新的 perimeter，以及身份和内容是最重要的参数，当我们试图过渡到一个工作在当今IT世界的数据安全模型时。我们需要改变我们考虑安全的模式。在平台上完全采用硬件或固件（有时甚至是软件）的情况下，可能无法在加密密钥中进行。因此，我们需要在移动数据安全方面做出重大改变，以便可以考虑移动数据安全。
A New Authentication Paradigm?

WITH THE PROLIFERATION OF THE CLOUD, an old issue has resurfaced: seamless authentication and authorization to remote services. This concern has been around for many decades, with the development of protocols like Kerberos and tools such as IKE and AD. However, none of these protocols truly solved the overall problem.

User-ID/password is without a doubt the single most used and trusted method to achieve authentication and authorization. However, this method has proven to fail more than we would like to admit. Services offered by Microsoft, Google, Amazon and Facebook are increasingly revered by other Web services as trusted, using them as a sort of public key infrastructure (PKI), though all are based on user-ID/password. Why is this?

The answer is administrative simplicity. All other methods require more resources or a higher level of user complexity. The user-ID/password method, despite its unreliability and possibility of user negligence, is cheap—often zero cost, compared to other methods.

Central allocations and revocation are too complex, and the responsible security staffers simply hope the user will not misuse any access privileges. Still, statistics say 80 percent of all IT crimes are internal, reminding us that opportunity often creates the criminal.

In the age of the integrated cloud, perhaps it’s time for a paradigm shift—a new multiplatform, authentication technology that would support system owners and allow administrators to maintain access control while utilizing the proper tools (without using external services).

How can this be done? Let’s face it: the technology has been around for years, such as private/public keys and PKCS#12 certificates. We just have to tweak some protocols and tools to make this shift. For starters, we can use trusted certificate data to validate organizations. From there, individual keys can link individuals to the organization.

Can it be done? Yes, it can be done. In fact, it already has been done, though most of us don’t realize it. The model design for this type of tool is called Factorum. Factorum was the authentication and authorization process for the AT&T Plan9 Operating System (OS) from the early 1990s. Factorum works a lot like SSH and IPsec public/private key processes, but it’s not a part of the operating system. Rather, it sits on top of the OS, and controls a single user’s access to the complete system. Designed for a distributed, multiserver environment, it supports all protocols we can encounter, not just Web ones.

Plan9 and Factorum are no longer available, but by adding Factorum-like functionality to the current PKI/AD and allowing local and remote systems, as well as protocols like SAML2 to work with public/private keys instead of current identity parameters, we get a simplified functionality. This allows local system owners to control access by distributing public keys and revoking access by deleting the private ones.

By mimicking Factorum’s role-based authorization, we could give the user the right access in the same way local AD installation would be accessed. We could then have a trustworthy, boundless single sign-on authentication/authorization without multiple passwords or costly two-factor authentication tools. (3C)

Lars Magnusson, CISSP, is an information security manager in the Swedish automotive industry. He is based in Trollhattan, Sweden and can be reached at l.magnusson@home.se
In a sea of IT professionals, ISACA members get noticed.

Many IT and information systems professionals worldwide consider membership in ISACA essential to their career advancement. As a nonprofit, global association, ISACA connects exceptional people with exceptional knowledge to provide members with a robust offering of professional resources.

Get recognized—our members do.

www.isaca.org/benefits-infosec
Receive a new webcast each week.

(ISC)² members must stay current in the evolving world of software security. This series of webcasts will provide you with a new webcast each week focusing on securing a different phase of the software lifecycle. It will show you what security measures need to take place at the beginning in the requirements phase, how security must be built in the design phase, and how to test if the application is resilient enough to withstand attacks in the testing phase.

Also, this series will feature a webcast on the value of the CSSLP and how to study for the exam.
The Fusion Of Logical And Traditional Security

September 10-13, 2012 • Philadelphia, PA

What You Can Expect

- 220+ conference sessions available throughout 25 education tracks
- Exclusive (ISC)² Town Hall and Member Reception
- Free 1/2-day credential clinics on Sunday for CISSP®, CSSLP®, CAP® and SSCP®
- 2-day official education programs for CISSP and CSSLP
- 2-day technical programs on cloud security and digital forensics
- Impressive lineup of keynote speakers
- International Government Summit
- CPEs for attending the conference

www.isc2.org/congress2012

Visit the website for more information and special pricing (members must register through the site).