EXPANDING EDUCATIONAL OPPORTUNITIES IN ASIA

THE FIRST 48 INCIDENT RESPONSE HOURS

Malware Analysis 101

Are You Satisfied with Your Job?

5 Minutes with Australia’s Greg Mazzone
A DDoS ATTACK JUST ATE $16M IN REVENUE. ALONG WITH HIS ANNUAL BONUS.

ALI CARTER // CIO

FEATURES

› MANAGEMENT

16 The First 48 Hours
Incidents happen. How you initially respond to them can make all the difference. BY COLLEEN FRYE

› TECHNOLOGY

22 Cracking a Compromise
Dissecting the malware that invaded your system can protect you from future attacks. A member shows you how to do it. BY ‘GRECS’

› PROFESSIONAL DEVELOPMENT

30 Building a Bigger Pipeline
The 2015 (ISC)² Global Information Security Workforce Study shows we must funnel more people into information security...and soon. Plus, highlights of key findings. BY ANNE SAITA

Illustration (above) by ©ENRICO VARRASSO

A malware analyst outlines tools you can use to tear apart malicious code. PAGE 22
Editor’s Note

FINDING COMMON GROUND

One of the most difficult aspects of editing a magazine for a large, global membership is creating content that will appeal to all skill levels and different disciplines.

I love hearing from members when an issue is published; especially suggestions for articles and offers to pen a piece based on that member’s expertise or interest in a security issue. Truthfully, though, those emails typically are few and far between.

So when we received a report on InfoSecurity Professional magazine based on a recent membership survey, our staff was excited to find the publication remains one of the most popular benefits in the growing (ISC)² portfolio. Some thought the material was too technical at times; others, not technical enough. Some liked the length of features; others found them too long or too short. Some confused us with another great (ISC)² publication, the more technical peer-reviewed (ISC)² Journal. Some admitted they never read an issue.

The vast majority of comments, however, said that we were doing a good job.

There are a lot of other digital publications in the security space. Most focus on technical issues. InfoSecurity Professional, however, as its name implies, takes a broader approach that includes management and professional development articles that help you do your job better—maybe even land a much-deserved promotion. This organization has a tremendous amount of talent within its membership, and we at the magazine want each of you to expand your influence within your company and your community.

We love showcasing your talents and sharing your knowledge, whether as an article’s author or expert resource. If you have an idea for an article—something we haven’t tackled or a perennial topic viewed from a new perspective, please contact me at asaita@isc2.org.

And thank each of you who took the time to fill out the membership survey and to let us know where we can continuously improve.

› ANNE SAITA

ADVERTISER INDEX

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

Neustar.........................................................2
MIT.............................................................5
(ISC)²..........................................................7
Capella.......................................................13
EWF..............................................................15
(ISC)²........................................................21

McAfee......................................................26
(ISC)²......................................................27
CyberArk.....................................................28
ISACA.........................................................35
Twirling Tiger Press.................................37

©Rob Andrew Photography
“There are two kinds of companies today. Those that have experienced a security breach and those that don’t know it yet.”

Howard Shrobe
Director, Cybersecurity, MIT CSAIL

Cybersecurity starts with you. Become part of the solution.

Join the new online Cybersecurity course at MIT starting September 15 and save 10% using code ISC10.

MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) presents a six-week online course that examines Cybersecurity challenges in:

- Hardware security architecture
- Resilient Software
- Public Key Cryptography
- Cybersecurity Policy

Learn the latest developments and research to help your organizations move from ‘patch and pray’ defenses to security ‘by default.’

REGISTER TODAY MITPROFESSIONALX/MIT.EDU
MEETING THE NEEDS OF THE ASIA-PACIFIC MARKET

When I first took over the Asia-Pacific operations for (ISC)²® in 2002, our focus was to spread the word about the organization and about the doors our certification and educational programs could open for people.

Today, we have 12,000 credential holders throughout the region who’ve met and continue to maintain the high standards of our certification programs. I anticipate that the member base in this region will continue to increase to help meet growing demand for more global information security professionals.

Every region has its challenges, and for us, one of the biggest is trying to support and grow our profession in a vast region with a broad mix of markets and diverse cultures, where perceptions of information security differ. (ISC)² wants to establish a universal, common framework of understanding and a baseline for the interpretation of what information security is, relevant to the ever-changing threat landscape that knows no cultural and geographical bounds. Recently, we launched new certifications, the CCFP, CCSP and HCISPP, in response to the need for specialists in the information security domain.

For better or worse, a lot of what we do is driven by legislation in the respective economies. There are different interpretations, but the end goal is always the same: ensure and maintain confidentiality, integrity and availability (CIA). That’s precisely where we need the most investment in technology and capacity-building.

The Asia-Pacific region faces several challenges when it comes to growing and maturing the information security industry here. Some economies within the region have not had exposure to the broad range of information security topics covered in the CISSP, for example. Also, few universities offer formal information security education. These factors present a great opportunity for (ISC)² to continue to engage practicing professionals and help them to share their information security knowledge to overcome these challenges.

But despite these differences, all of our existing members are bound by a strong desire to improve both their careers and their companies; a discipline that has proven to be beneficial to individuals and economies alike. The discipline is known as Continuing Professional Education (CPE) credits. This requirement is a good measure to ensure individuals remain current (where possible) amidst evolving industry trends and technologies.

This also helps us as an organization and as a region to work to “professionalize the profession” as we like to say. Our members in the region also have a passion for raising cybersecurity awareness through the (ISC)² Foundation’s Safe and Secure Online program, available since 2006 in Hong Kong and soon in India. In total, the program has helped over 165,000 children worldwide learn how to protect themselves online and become responsible digital citizens.

We have a huge opportunity in the coming years to push for capacity-building and to invest in infrastructure and workforce. An immediate example will be preparation for the 2020 Summer Olympics in Tokyo. Of course, that’s just one country, but that enormous project may create a ripple effect that can help more Asian markets see the value in investing additional information security resources and awareness so (ISC)² members have more opportunities to influence the security posture not only of their organizations but of their economies.
(ISC)² and the Cloud Security Alliance (CSA) are excited to introduce the Certified Cloud Security Professional (CCSP), a new credential developed to meet a critical market need to ensure that cloud security professionals have the required knowledge, skills, and abilities to audit, assess, and secure cloud infrastructures.

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

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

Brought to you by (ISC)² and CSA cloud security alliance

www.isc2.org/ccsp
MEMBERS CAN NOW TAP INTO COMPLIANCE DATABASE

(ISC)² MEMBERS NOW have discounted access to the Unified Compliance Common Controls Hub, a massive data repository of global laws, standards and other compliance-related regulations, thanks to a partnership with Unified Compliance, the developer of the only patented compliance database framework.

The portal provides (ISC)² members with rapid access to more than 90,000 individual mandates from 800-plus laws and standards from around the globe. The tool helps members compile custom control lists by vertical industries, market segments and geographies. When members subscribe to the Hub, they will receive a 10 percent rebate off the normal subscription fee.

“We are proud to include discounted access to the Hub in our continually expanding portfolio of member benefits,” says (ISC)² Director of Membership Relations and Services Erich Kron, CISSP-ISSAP, HCISPP. “We hope the Hub will help many of our members in their daily jobs by providing them with a convenient platform to streamline and assess policies and procedures as they relate to the myriad of complex regulatory requirements.”

Accessible at isc2.CommonControlsHub.com, the portal reinforces (ISC)²’s ongoing mission to provide the latest industry information and professional tools to its global network of dedicated information security professionals in support of their career objectives.

The Hub is available as a free compliance research tool for users to research up to five authority documents at a time. Subscriptions to (ISC)²’s Common Controls Hub are based on common controls access, custom compliance template creation and number of users. Corporate subscriptions for (ISC)² members start at $4,496.

SECURITY CONGRESS SESSIONS ANNOUNCED

Sept. 28 – Oct. 2
Anaheim Convention Center

Ready to plan your trip to Anaheim, or still riding the fence on whether to attend this year’s Security Congress? Then be sure to check out the list of sessions and speakers on the (ISC)² Website.
The Honorable Jejomar C. Binay, vice president of the Republic of the Philippines, will keynote APAC’s (ISC)² Security Congress, taking place July 28 and 29 at the Sofitel Philippine Plaza in Manila. Information security experts from government, industry and academia will provide two days of hands-on technical workshops and discussions led by global and regional industry speakers on emerging threats, best practices and solutions to challenges.

“The conference will include keynote addresses, regional roundtable discussions and sessions in management and strategy and technical tracks.”

The conference will include keynote addresses, regional roundtable discussions and sessions in management and strategy and technical tracks. Topics will cover professional development, information security governance, supply chain security, cloud security, business continuity management, Internet of Things, mobile security and digital forensics.

One highlight will be a regional roundtable discussion from 11:30 a.m. to 12:30 p.m. on Tuesday, July 29, on “Challenges in Critical Infrastructure Protection” featuring information security experts from Australia, Korea, Hong Kong, Singapore and India. There is also a hands-on forensics workshop from 3:45 to 5:15 p.m. on Monday, July 28. Other notable sessions include “Security and Adoption of IPv6: Impact on Your Security Posture,” “Capacity Building—Lessons from (ISC)² Global Information Security Workforce Study” and “Peace and Order in Cyberspace.”

In addition to Vice President Binay, event speakers include Voltaire T. Gazmin from the Philippines’ Department of National Defense; (ISC)² CEO David Shearer; Prof. Corey Schou, an (ISC)² co-founder and current chairman of the board; board members Howard Schmidt, Freddy Tan and Dave Lewis; Prof. Jill Slay of the Australian Centre for Cyber Security at the University of Australia; Wan Suk Yi, a senior researcher for the South Korea Internet and Security Agency; and Darren Cerasi, director of i-Analysis in Singapore.

Last year, more than 350 people attended the event. Details about the (ISC)² Security Congress APAC 2015 program are available at http://apac-congress.isc2.org. (ISC)², NDCP and NDCPAAI members are eligible for discounted pricing.

For the second year in a row, the CISSP was named the ‘Best Professional Certification Program’ during the annual SC Magazine Awards US at the RSA Conference in San Francisco in April. The CISSP was also chosen as the ‘Best Professional Training/Certification Programme’ for the SC Magazine Awards Europe at the Infosecurity Europe Conference in London in June.

“With the nature of today’s evolving threats, it’s more important than ever to combine an educated workforce of security experts with process and technology. (ISC)² is setting the standard of excellence in the Best Professional Certification Program,” says Illena Armstrong, VP of Editorial for the security magazine.

A panel of judges comprised of recognized security professionals and leaders from a variety of backgrounds and vertical markets chose the 2015 Professional Award winners. The rigorous judging process includes testimonials, industry assessment and additional research.
SPEAKER PUBLISHES CYBERSECURITY THRILLER

No doubt the mass media is waking up to the potential of cybersecurity—as a plotline. One of the newest entries to the genre is The Florentine Deception, a self-published cyber thriller written by (ISC)² speaker and Symantec Fellow Carey Nachenberg. As one of the co-authors of Norton Security and Symantec’s senior-most engineer, Nachenberg used his vast experience to write a novel about a cybersecurity expert who unearthed a mystery while rummaging through an old PC.

He plans to donate the proceeds from book sales to charities benefitting underserved students and veterans. His goal is to donate at least US$10,000 to KIPP.org, NPower.org, Success Academy, UniCamp and UCLA computer science scholarships to low-income students.

Learn more at www.florentine-deception.com.

(CSC)² SECURITY CONGRESS EMEA MARKS SECOND YEAR WITH EXPERTS FROM NOTABLE AGENCIES, COMPANIES, INDUSTRIES

THE INFORMATION SECURITY community from Europe Middle East and Africa (EMEA) will come together in Munich to share knowledge and frontline experience at the second annual (ISC)² Security Congress EMEA, October 20-21. The rich and diverse speaker program will help attendees examine how company and government strategies are maturing to ensure resilience and get ahead of requirements.

The conference program features more than 40 educational sessions from practicing experts and frontline professionals working across management, operational and specialist disciplines. The event also offers plenaries and interactive sessions to encourage insights from delegates, as well as the opportunity to register for up to two-pre-conference, half-day workshops.

Notable sessions include:

- Current Threats and Collaborative Strategies in Cyber Security
- Counting the Stars, but Losing the Moon—Securing the Internet of Things
- We Are Visiting the Cloud, Are You Joining?
- The Myths in Biometrics
- How a CISO May Deal with the New European Privacy and Security Legal Instruments
- Cyber Money Laundering: Are We Getting Better at Chasing Dirty Money?

More information, including the full program, is available on the Congress website.

CPEs

When submitting CPEs for (ISC)²’s InfoSecurity Professional magazine, please choose the CPE Type: “(ISC)²’s InfoSecurity Professional Magazine Quiz (Group A Only),” which will automatically assign two Group A CPEs.

FIELD NOTES

SPOTLIGHT:
(ISC)² RALEIGH-DURHAM, N.C. CHAPTER

CHAPTER LEVERAGES UNIVERSITIES, GROWING TECH INDUSTRY

With more corporations moving into the Raleigh-Durham area because of its temperate climate, affordable housing and access to world-class universities, the (ISC)² Raleigh-Durham Chapter sees opportunities to build membership and help future cybersecurity professionals.

“The demand for information security professionals is increasing at a rapid pace, and that includes in the Raleigh-Durham area,” says Chapter president KC Udoh. “We’re seeing more companies move their headquarters or divisions here and set up security operations centers.”

The Chapter currently has 47 members, almost all of them credential-holders. Because a competing organization with deeper community roots focuses its meetings on training and education, the Chapter leadership agreed to promote professional development and share tips on timely technical issues.

Between 25 and 50 people attend the bimonthly meetings, including recruiters who announce employment opportunities and better understand the caliber of (ISC)² credential holders, Udoh says. At recent meetings, members have posted job openings on a mobile bulletin board, including contact information for personal connections at those companies.

The area is home to Duke University, North Carolina State University and the University of North Carolina-Chapel Hill. In addition, there are campuses for Strayer University, DeVry University, and ITT and other technical institutes.

“We are hoping to build a critical mass so we can offer scholarships and give back while also providing these future information security professionals with valuable connections in the industry,” Udoh says.

Last September’s meeting included a representative from Toastmasters giving public speaking pointers, temp agency personnel discussing job trends and a professional photographer providing headshots for LinkedIn profiles. This September, the group plans to hear a life coach speak about work-life balance.

Udoh jokes that the meetings feel a little like group therapy, in that everyone bonds over common issues and works together to become better people. “You make friends during these meetings,” he says.

According to Verizon, an estimated 95% of espionage attacks involved phishing.

Nearly 80% of all malware attacks come from phishing attempts.

Source: ThreatSim’s Annual State of the Phish Report
MEMBER FOCUS ON WELLNESS

HERE’S MORE TO professional success than mastering technologies and management techniques. It also takes effort to remain or maintain mental, physical and spiritual wellness. We encourage members to share about different types of yoga, meditation, wellness and fitness activities they practice to remain sharp, empower themselves and manage their daily routines.

In this issue, (ISC)² member Pararajasingam Jegatheeswaran shares some yoga practices he follows to maintain his work-life balance and a healthy, happy life. PJ is currently based in Hong Kong and believes active engagement in health and wellness activities not only helps maintain a healthy body but is the basis of everyone’s happiness and peace.

Here are links to two yoga practices he recommends for those who wish to get started or to expand their own personal wellness program.

Activity 1: Isha Yoga  
Country of Origin: India  
Web Link: http://www.ishayoga.org/  
Popular You Tube Link: https://www.youtube.com/watch?v=gDdUNeK7JW-g&list=PLfUGp2y5JhADF1JSC-zVD4PqNAJK-WNi

Activity 2: Body and Brain Yoga  
Country of Origin: South Korea  
Web Link: http://bodyandbrain.ca/wp/  
Popular You Tube Link: https://www.youtube.com/user/IlchiLee

Have another tip to share with other members? Send a brief summary, along with your name and location, to infosecproeditor@isc2.org.

(ISC)² EXPANDS PRESENCE IN D.C. REGION

If you work in information security, there’s a good chance you or your employer are located in one of five regions of the United States, according to the 2015 (ISC)² Global Information Security Workforce Study (GISWS).

One of those regions is Washington, D.C., where (ISC)² membership has grown to 13,500 and where (ISC)² recently set up a corporate office.

“Our members are those on the front lines in D.C., who are being asked to help solve the nation’s most complex cybersecurity challenges,” says Dan Waddell, who was named managing director of the National Capital Region in 2014.

“As the U.S. government’s investment in cybersecurity increases, we need to make sure that our members have a direct pipeline to those who influence change, that they are equipped with relevant and timely information, and that their voice is being heard throughout the legislative and policy communities. As the managing director, I will be directing resources for their benefit and on their behalf.”

“Everyone in this room has a hacker inside them. Everyone feels that people are keeping things secret that shouldn’t be kept secret. But you have to step back and ask whether any of us has the right to judge what private information can rightfully be exposed.”

—ALEC BALDWIN, actor, closing out the 2015 RSA Conference in San Francisco
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
CHANCE FAVORS THE PREPARED MIND

AS I GEAR up for my quarterly Incident Response Readiness testing, a “live fire” exercise run jointly with my penetration test team, I am reminded of a quote by the late Gen. Alexander “Archie” Vandergrift:

“Positions are seldom lost because they have been destroyed, but almost invariably because the leader has decided in his own mind that position cannot be held.”

So much of the recent media focus, perhaps driven by the high-profile breaches of late, seems to be centered on the “assume you are owned” mentality of the security practitioner. I find this sense of resignation disappointing at best, self-destructive at its worst.

After 20 years in this profession, I understand the sense of resignation many of us feel. I have felt it myself, but over the past two decades, I have found that it moves in cycles. It waxes and wanes following the news, or politics, or even our own professional ups and downs. But there is a way off of the wheel. It comes from understanding human nature, and, more importantly, the boundaries of your sphere of influence versus your sphere of control.

As practitioners, we often focus on the latter, but it is the former where we may have the most leverage. This is especially true if we look at our incident response preparedness exercises as a chance to reach out and build relationships with those individuals we will need most later.

Perhaps it is human resources, or your legal department…maybe corporate communications. Regardless of the function, by recruiting others into to your exercises, you establish relationships and increase your visibility of security into areas frequently lacking awareness of such matters. You can now begin to drive awareness through the real-world scenarios you develop in your exercises, shaping the behavior of others through inclusion and participation instead of just boring security awareness training. This creates a force multiplier.

So, while you may have seen this movie before (and you think you know how it will end), you have more control over the outcome than you imagine. By working horizontally and vertically within your organization, you can gain valuable mindshare around your goals and capabilities, which will pay dividends for a long time.

By working horizontally and vertically within your organization, you can gain valuable mindshare around your goals and capabilities, which will pay dividends for a long time.

So, as you begin your own incident response testing, just remember these wise words from Ralph Waldo Emerson:

“A great part of courage is the courage of having done the thing before.”

Remember, we have been here before, and we will be here again. Have the courage. Until next time, I look forward to continuing the conversation. ☑
EARN UP TO 19 CPE CREDITS
BUILD A NETWORK OF THE MOST DYNAMIC WOMEN IN OUR INDUSTRY
TAKE HOME TOOLS, BEST PRACTICES & SOLUTIONS TO ACHIEVE SUCCESS

Women of Influence Awards
Nominate your peers, clients and customers for the Women of Influence Awards. Co-presented by CSO Magazine and Alta Associates, the awards honor four women for their accomplishments and leadership roles in the fields of security, risk management and privacy.
Winners will be announced at a ceremony during the EWF event.
FOR NOMINATION FORM GO TO: www.ewf-usa.com
Nominations must be submitted by August 15, 2015

Big Data, Big Risk, Big Opportunities

From the Keyboard to the Boardroom—A World of Opportunity at your Finger Tips
Suzanne Vautrinot - Major General & Commander, US Air Force (retired) and Board of Director Member, Symantec, Wells Fargo and Ecolab

Denial of Reputation: Sensible Security PR

Opportunities and Innovation in Healthcare Big Data

Data Sovereignty, Global Cybersecurity Policy & Government Control

Voice Privacy Conundrum

Strategic Look at Nation State Cyber Attacks

The Data You Want—An Inside Look at Monitoring and Alerting

For more information on the EWF or to register, please visit: www.ewf-usa.com
“Suspicious activity on the network!” This alert from one of your IT staffers will set in motion a series of activities that can impact your organization’s future. What you do next is critical…and the clock is ticking.

“The first 48 hours are the most crucial,” says Edward McCabe, principal consultant at Rendition InfoSec LLC, which specializes in penetration testing and incident response. That’s when you have to contain a potential breach, control the message that goes out (or not) to the public, keep on the right side of the law and ultimately minimize disruption to your business and customers.

That’s also when “you have the advantage over attackers if you do incident response properly,” adds McCabe’s colleague Jacob Williams, principal consultant at Rendition and the SANS Institute’s lead on digital forensics and incident response. “The attackers assume you don’t know they’re there.”

To maximize those 48 hours, there are key steps to take. We’ve assembled advice from experts in incident response, compliance, legal and law enforcement. The one thing they all agree on is the importance of advanced planning.
ACTION ITEM 1
ASSESS THE INCIDENT
BEFORE YOU ACT

Detection, identification, containment, eradication and closure are the industry standard steps an incident response (IR) team should follow, says Keith Fricke, CISO at Mercy Health based in Cincinnati, Ohio. The nature of an incident—from a virus outbreak to a stolen laptop to a network intruder—and the type of data potentially at risk determine the specific course of action, he says.

Having an IR plan in place is key, urges Phil Burdette, senior security researcher at Dell SecureWorks. First and most important, you should know what the business is trying to protect, he says. Then identify and assess the people, processes and technology involved, the key stakeholders, what technology can be leveraged, who will make decisions, the communication intervals and when senior management will get reports. “It’s like organized chaos.”

Burdette warns that it’s important to keep in mind that the incident may not be an isolated event but rather part of a larger intrusion. “That event may be the tip of the iceberg.”

And locking down the network may not always be the appropriate response. Capturing memory is critical, he cautions. “Shutting a system down could potentially destroy evidence. We have to work closely with legal and follow best practices to ensure our case could stand up in court.”

Not every incident is determined to be a breach, so “you don’t want to raise unnecessary red flags until you get all the facts,” Fricke warns. “[IR’s] job is to present the data and information,” says Burdette. Fricke adds that the IR team needs to notify internal leadership that an investigation is going on and keep them posted as they collect the facts. If they confirm a breach has occurred, “the IR team takes on a different shape.”

At that point, IR brings in legal, compliance, risk management and public relations teams, “and you may contract with a third party to do forensics. Over that subsequent 48 hours, the legal department works with the PR people to ensure the right communication is going out to the right people at the right time.”

Fricke suggests you may want to gear up a call center to answer questions from the public. “And there are companies that specialize in helping companies set up a program for credit monitoring.”

ACTION ITEM 2
KNOW THE LAW

It’s important to distinguish “incident” from “breach,” cautions Benjamin Wright, attorney and SANS Institute instructor. “Rarely when you discover something do you have enough evidence to conclude you have a legal breach. The thing you have, before evidence of a legal conclusion of a breach, is called an ‘incident.’ That’s where things start.”

According to Wright, first, you need to do something to stop the damage. Then, investigate what happened, he says, adding that confidentiality is paramount. “That investigation is very sensitive from a legal perspective. Legal counsel can lead the investigation from a legal perspective. Counsel...
can designate the investigation an ‘attorney work product,’ which is like attorney-client privilege.”

This confidentiality is crucial, he says, because when legal counsel and management review the evidence, they may conclude that there was an incident, “but we don’t have evidence that rises to the point of a breach. Therefore, we’re not going to give notice to the public.”

The “attorney work product” designation will also keep your investigation from falling into the hands of legal adversaries who could second-guess or sue you, Wright adds. These “adversaries” could include government agencies, states’ attorneys general, Visa, your bank, or other banks that might sue you for credit card breach. “So ‘attorney work product’ can be a very valuable and strong tool for protecting the confidentiality of your investigation.”

Also important is knowing the data breach law for your industry and jurisdiction, declares William C. Snyder, former federal prosecutor and visiting assistant professor of law at the College of Law at Syracuse University. At the federal level, the SEC, FTC and FCC have data-breach rules in place, but the U.S. Congress has not passed a law yet with regard to personally identifiable information (PII), he says. Most states have passed their own data breach laws, but “you’ve got to know which statute you fall under because there is no uniformity.”

Snyder also warns against breaking the law in the course of your incident investigation. “Hack back is illegal,” he warns. If you go after the intruder and enter their network, it’s considered a federal felony. You’re not authorized to access someone else’s computer just because you’re trying to figure out who they are.

Organizations also need to be careful of the Wiretap Act, he says, which covers real-time communication. That can include voice messages, code coming into your machine, etc. “The fact that you own the computer doesn’t mean you’re entitled to the communication.” If you don’t have knowledgeable people in this area, Snyder advises hiring a third party since the Wiretap Act says that you, as a company, can’t intercept communication that isn’t intended for you.

**ACTION ITEM 3**

**DEPLOY YOUR PREPARED ACTION PLAN**

“Preparation is key to minimizing the impact of a breach,” says Troy Leach, CTO of the PCI Security Standards Council (SSC) in Wakefield, Mass. “Similar to the way a fire drill offers the opportunity to test your action plan in an emergency, PCI DSS requires that organizations have a plan in place, along with prescriptive steps to execute against that plan.” He encourages organizations to regularly evaluate their plan to make sure that key elements—people, process and technology—have not changed. “It is imperative to update your response plan any time there is a significant change to your organization.”

You also need to verify that the controls you put in place are working as you expect them to. “Practices, such as vulnerability scans and penetration tests, help you see where the vulnerabilities are that could allow criminals to steal sensitive information.”

**...DISTINGUISH “INCIDENT” FROM “BREACH”...**
The PCI Council recently released guidance to help organizations maintain a pen-testing methodology. If you confirm a breach has occurred and your organization handles credit card data, Leach advises, “the first thing you should do is reach out to the payment brands and the Secret Service. Payment brands have…step-by-step procedures in the case of a breach.”

“Security professionals and law enforcement will want to pinpoint where the intrusion occurred in order to contain and eliminate the threat and to prevent putting further data at risk.”

—TROY LEACH, CTO, PCI Security Standards Council

Organizations with compliance mandates such as PCI DSS or HIPAA should also “be sensitive not to destroy the environment in which the breach occurred,” he says. “Security professionals and law enforcement will want to pinpoint where the intrusion occurred in order to contain and eliminate the threat and to prevent putting further data at risk.”

**ACTION ITEM 4**

**CONTACT LAW ENFORCEMENT**

Before you ever need to call law enforcement, learn who the appropriate agency is for both your industry and geographic area, former prosecutor Snyder advises. “You can’t just dial 911.” In some cases, you will call the FBI, but your local or state police may have expertise. Other industries fall under Secret Service or Homeland Security, he adds.

Once you know the appropriate local authorities, identify one or two key people in your organization who will be the primary contacts, offers Joseph R. Bonavolonta, assistant special agent in charge with the Boston Division of the FBI, overseeing the Cyber, Counterintelligence and Security Branch.

The decision to bring in law enforcement is up to the individual organization, but he says three primary scenarios might well require FBI involvement:

- When proprietary information or data is on a hosted server and the organization doesn’t have the means to take it back
- When an imminent and ongoing threat such as DDOS is so onerous that it’s impeding the operations of the company
- When your IT department has identified an insider threat
Once the FBI gets involved, Bonavolonta explains, they will put together a team that includes a cyber-trained case agent, a computer scientist, a forensic examiner and, most likely, an intelligence analyst. From your IT department, the FBI will expect to receive specific dates and times of the incident, IP origination, log files, domains, etc., and the specific intellectual property that was compromised.

Business continuity is a priority for the FBI, Bonavolonta emphasizes. “We understand the ramifications if a company’s business operations have to be shut down, and there are things we can do to mitigate that.” For example, “If there’s an intrusion or breach, we recommend the company isolate the infected network and capture or make some image of that network, either separately or offline. The victim company can do that themselves, but we’d like to be called in to do it for evidentiary purposes.” Also, he recommends being very cognizant of interactions with third parties. “If you’re a victim of a malware attack, even if a system is isolated, the malware can enable a back door through third-party vendors.”

EXPERT ADVICE

by Colleen Frye

Beware of the Traps and Pitfalls in Incident Response

Avoid a DIY response. “If you’ve never exercised an incident response plan before, you don’t want to try it out [during an incident],” says Rendition’s Jacob Williams.

Fix the problems you’ve identified. “The purpose of compliance is to create a secure environment,” says Troy Leach of the PCI Security Standards Council. “Security professionals need to evaluate not only where the intrusion occurred but why the security controls failed. If your environment is not secure, you must identify the problem and fix it so the criminal can’t repeat the attack.”

Don’t let intruders know what you know. “Often, [organizations] will immediately stand up a war room and send out communication to appropriate parties, but that communication occurs on the corporate infrastructure,” says Phil Burdette of Dell SecureWorks. “We don’t always know what level of access the threat actors have. For all you know, they may be conducting counterintelligence. Having an out-of-band communication plan is integral. We don’t want adversaries to know what we know.”

THE CLOCK MAY BE TICKING ON YOUR INCIDENT RESPONSE, BUT OUR EXPERTS CAUTION YOU ABOUT SOME COMMON MISTAKES.

Notify management in a timely manner. “It’s a common mindset for tech-minded IT staff to drill into problems deeply before they raise the flag on something,” says Keith Fricke of Mercy Health. “There needs to be some balance between how much time they’re taking to collect the right information and when they notify management.”

Be aware of the sensitivities. “The legal conclusion that a breach has occurred is a highly subjective idea,” says Benjamin Wright. “Reasonable people can look at the same evidence and reach different conclusions. That’s why an investigation is so sensitive. A good investigation requires lots of work and analysis.”

Once the FBI gets involved, Bonavolonta explains, they will put together a team that includes a cyber-trained case agent, a computer scientist, a forensic examiner and, most likely, an intelligence analyst. From your IT department, the FBI will expect to receive specific dates and times of the incident, IP origination, log files, domains, etc., and the specific intellectual property that was compromised.

Business continuity is a priority for the FBI, Bonavolonta emphasizes. “We understand the ramifications if a company’s business operations have to be shut down, and there are things we can do to mitigate that.” For example, “If there’s an intrusion or breach, we recommend the company isolate the infected network and capture or make some image of that network, either separately or offline. The victim company can do that themselves, but we’d like to be called in to do it for evidentiary purposes.” Also, he recommends being very cognizant of interactions with third parties. “If you’re a victim of a malware attack, even if a system is isolated, the malware can enable a back door through third-party vendors.”

FINAL ACTION ITEM

REASSess AND TAKE THE LONG VIEW

Understanding the incident response, compliance, legal and law enforcement aspects of responding to a breach before it happens is something all the experts stress. “Being prepared for a breach is really important,” says Fricke. “Having some documented procedures in place helps you make better decisions under duress. Not being prepared may cause you to make mistakes when an event happens.”

And while the first 48 hours are important, detection, identification, containment, eradication and closure can be a lengthy process. “Oftentimes, it’s a marathon, not a sprint,” says Burdette. “It’s easy to get burned out in the first 24 to 48 hours. Incident response may go on for weeks at a time. Recognize that you [may] need to be prepared for a longer-term engagement.”

COLLEEN FRYE is a freelance writer based in Massachusetts and previous contributor to InfoSecurity Professional.
Join us for the Fifth Annual

SECURITY CONGRESS 2015

Sept. 28 - Oct. 1 • Anaheim, CA • Anaheim Convention Center

REGISTER TODAY

ADVANCED PRICING
OPEN UNTIL AUGUST 31, 2015

EARN UP TO 62 CPEs!

Sessions include:
» The Anatomy of a Cloud Data Breach
» Security from the Trenches – Scrying Security
» Passive Information Leakage: A New Threat to Sensitive Business Information

View the full list of sessions at (ISC)² Security Congress 2015.

Tracks include:
» 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
» People Centric Security

REGISTER TODAY
congress.isc2.org

© Copyright 2015. (ISC)², Inc. All rights reserved.
Your system has been compromised. Data has been stolen or destroyed, and it appears that site security has failed. And you think you’ve pinpointed the culprit: malware.

Now, it’s time to figure out the who, when, what and, perhaps why the incident occurred. The best way to decipher these riddles is by parsing the malware—getting to know it inside out. Hopefully, by gaining this intimate understanding, you can prevent future compromises.

Malware analysis plays a critical role in helping defenders understand the effects of past compromises and improve their security posture against future attacks. That’s why it’s important for organizations and individuals to develop a basic capability that can fill this gap—malware analysis.
**POST-MORTEM BASICS**

Malware analysis is loosely defined as “reverse engineering of malicious software in order to understand how it works and what it does.” The environment for analyzing malware often includes one or more sandboxed environments with applications for monitoring operating system activities. Analysts typically use virtualized systems due to their ease of management; however, physical machines may be necessary in certain situations.

Automated analysis solutions provide another option for dealing with large sets of malware samples. Depending on the goals of a specific analysis, a single sandboxed machine is usually adequate, but another machine may be necessary to emulate a network the malware may be expecting.

In general, the malware analysis process consists of three stages: triage, dynamic analysis and static analysis (see Figure 1, below).

- **Triage,** the most basic of the steps, involves performing a quick ‘n’ dirty analysis to understand as much as possible about the malware.
- **Dynamic analysis** entails a bit more complexity and expertise and encompasses executing the malware and observing its activities within a controlled environment in order to learn how the malware acts during execution.
- **Finally, static analysis** involves disassembling malware down to its basic machine instructions and trying to piece together the logical structure and purpose of the code.

**ENVIRONMENT IS EVERYTHING**

In order to perform malware analysis, you need the proper environment in which to perform your investigation.

Standard platform options include either a virtualized system or a physical machine, depending on the complexity of the malware under the microscope. Virtual environments created with such products as VMware and VirtualBox are efficient and easy to set up, and they also create multiple snapshots that analysts can quickly revert to.

These platforms do not work well, however, when examining advanced malware that can detect the virtualized environment and subsequently terminate. That’s why having physical machines with disk reimaging software for these one-off situations is invaluable.

In analyzing the malware on either of these platforms, there are three main environment configurations: *automated analysis,* *single box analysis,* and *dual box analysis.* Depending on the situation, these options can fit into any of the triage, dynamic and/or static analysis phases.

Figure 2, below, represents a simple model that illustrates how different environmental options fit into the three phases of malware analysis.

**Automated analysis** is typically used in the triage phase, where software emulates user execution of and interaction with the malware. As the malware is executed and manipulated, built-in monitoring tools collect artifacts and present the results in a reportable format.

Automated analysis can either be performed online or in-house.

Online services offer convenient access to an automated
malware analysis sandbox for free or minimal cost. These services offer organizations the advantage of not having to maintain their own automated analysis environments. There is one caveat, however. Depending upon their service agreements, organizations may have to give up sensitive information to third parties in the process.

Several popular online malware analysis tools include Malwr.com, Anubis and ThreatExpert.com. For the risk-averse, many of these online providers also offer in-house options at various costs that ensure that analyses remain private.

Cuckoo Sandbox is one of the more popular in-house alternatives due to its strong analysis capabilities and open source licensing model. Setup can be difficult, but with a little bit of effort, it is a valuable and inexpensive option.

A single-box solution offers additional depth of investigation compared to an analysis sandbox. Not only can analysts use it to perform some of the basic triage steps, but it also forms a foundation for dynamic and static analysis.

The baseline of a single-box analysis environment should be established on an organization’s standard operating system, with a few additional tweaks to ensure the malware can execute properly. Most enterprises today use Windows 7 as a baseline, but for their analysis sandbox, they may make modifications, such as disabling automatic updates and other built-in security capabilities and foregoing their typical suite of security software.

You may need a dual-box solution, which includes a second system from which to monitor externally the analysis environment. When the monitoring tools exist on the same machine that the malware will be executing on, there is a chance of the malware sabotaging the results. The second box mitigates that risk somewhat and acts as a gateway for the single box, thereby recording an accurate account of what is occurring from an external perspective.

For those interested in creating a home lab, Microsoft also offers evaluation versions for most of their modern operating systems. The trials last 90 days before you need to register the product, which is more than enough time to determine if buying a full license is worthwhile. Modern IE, a browser compatibility testing resource from Microsoft, also offers some older operating systems, such as Windows XP, with the same 90-day expiration.

THE ANALYST’S TOOLBOX

Beyond the base operating system, understanding malware requires you to install a set of analysis applications. The three main categories of tools mirror the triage, dynamic and static analysis phases. The Internet is full of articles and blogs recommending the best tools for each of these phases; however, it can be overwhelming to know where to start.

For those new to malware analysis, the following are the most commonly suggested tools for basic analysis on Windows platforms.

**Triage**

- **Strings**: Extract ASCII and Unicode strings from binary files via the command line (free; Microsoft SysInternals)
- **BinText**: Extract ASCII and Unicode strings from binary files via a GUI (free; McAfee)
- **PeStudio**: Supports numerous analysis features
associated with indicators, virus detection, strings, imports, etc. (free for non-commercial use; Marc Ochsenmeier)

- PE Explorer: Unpack packed files and view executable properties
- OllyDump: Unpack malware through memory extraction via this OllyDbg plugin
- FileInsight: Hex editor geared toward malware analysis (free; McAfee)

**Dynamic**
- Process Monitor: Track and record processes (free; Microsoft Sysinternals)
- Process Explorer: Advanced Task Manager replacement (free; Microsoft SysInternals)
- Wireshark: Record and view network traffic (free; Wireshark Foundation)
- RegShot: Track Windows Registry and file changes (free)
- TCPView: View open network ports (free; Microsoft Sysinternals)
- FakeNet: Emulate network protocols such as DNS, HTTP, and SSL (free; Andrew Honig and Mike Sikorski)

**Static**
- OllyDbg: Basic debugging application used for extracting packed malware from memory and static analysis (free; Oleh Yuschuk)
- IDA Pro: Advanced debugging application (free for commercial use; Hex-Rays)

Additionally, depending upon the malware format, specialized tools may be available for tearing down and understanding specific file formats. Examples include PDFiD and PDF-Parser for analyzing PDF files, OfficeMalScanner for investigating Microsoft Office documents, and SWFTools for analyzing Flash files.

When setting up a single-box environment, establish a baseline, install the aforementioned triage, dynamic and static tools, and then re-baseline the known good image with a VM snapshot.

If you need a second box, generally, all that is required is a server configured to be the default gateway for the analysis sandbox machine. Depending on what you find through your triage and other analyses, typical services to run on this gateway could include DNS, HTTP and IRC. Netcat is also handy for creating ad-hoc listeners on any port on the fly. Other tools to install on the gateway include Wireshark to record any network traffic and Nmap to scan the analysis sandbox for open ports. REMnux from Lenny Zeltser offers all these capabilities and more, including many tools related to all three phases of analysis.

**DIVING INTO THE MALWARE**

Now that you’ve set up your analysis environment, you are ready to start analyzing malware. Regardless of the platform or environment, the basic methodology is the same: triage, dynamic and static analysis.

**Triage.** Triage allows an analyst to determine the basic runtime properties of the malware through automated analysis, hash comparison, file analysis and other specialized tools.

- Automated analysis involves running the malware through external or internal sandbox services for quick ‘n’ dirty results. The goal is to gain a rough understanding of the malware’s activities. Tools include both online and on-premise versions of Cuckoo Sandbox/Malwr.com, Norman, Anubis and ThreatExpert.com. For those interested in using an online service but do not want their samples distributed to others, Malwr.com offers a convenient option to keep samples private.
- Hash comparison involves computing the hash of the malware and searching existing services for similar samples. Although the automated analysis step may provide hash results, performing this activity on its
VirusTotal.com is the most common site for hash-searching, but other online providers offer similar services. These resources typically offer automated analysis-type capabilities as well, so if others submitted the malware, your organization can get the benefit of the analysis without having to submit the version affecting yours. Additionally, several tools, such as PEStudio, integrate with these services by automatically hashing the malware and searching for it on these services. Of course, another way of discovering if others are seeing the same malware is a quick Google search on the hash.

- File analysis provides additional insight into the file being analyzed. On its own, this step helps verify some of the previous triage steps while also providing additional data points.

File analysis often involves analyzing file properties to look for inconsistencies associated with the file type (e.g., a PDF file that is an executable), analyzing interesting PE header information such as odd DLL imports (e.g., a calculator app importing a network communication library), and finding interesting textual clues by extracting readable strings from binary files (e.g., host names and IP addresses). There are a number of tools that can be used in this area, but FileInsight, PEStudio, and the strings application go a long way.

If the analyst determines that the malware is packed, they must figure out the packing technique and reverse it before continuing the analysis. Standard tools exist for some of the common packers, but in other cases, the analyst can execute the malware and extract an unpacked version from memory. Tools for performing the unpacking step include PE Explorer and the OllyDump plugin for OllyDbg.

One final consideration you have to make during FOCUS 15 will offer a program packed with valuable and timely content on the ever changing security landscape.

Conference Highlights

- **90+ Technical Breakout Sessions**: Learn about the latest security innovations from Intel Security.
- **Networking**: Engage with some of the best minds in the industry.
- **Keynotes**: Hear from impressive industry leaders and security expert Christopher Young & Steve Grobman.
- **Other Conference Highlights**: Benefit from Targeted Group Meetings, a partner expo and much more.

As an ISC2 member, save $100 off your registration by using promo code FOCUS215 when registering!

Visit us at www.focus.intelsecurity.com/Focus2015/ to learn more.
file analysis is whether you need specialized tools for the specific file type you are examining. For example: PDFiD and PDF-Parser are useful for examining PDF files; OfficeMalScanner for investigating Microsoft Office files; and SWFTools for looking into Flash files.

**Dynamic Analysis.** After learning about the basic properties of the malware and deciding that further analysis is necessary, the next step is to observe the malware in action using dynamic analysis.

This process involves executing the malware and tracking modifications to various operating system characteristics, such as the Registry, files, logs, processes and network connections.

You may need to customize your analysis environment first, though. This involves taking the existing analysis sandbox baseline you’ve established and adding any necessary target software (e.g., Adobe Reader, Java, Flash, and browsers from sources like OldVersion.com and OldApps.com). Then you make any final configuration tweaks (e.g., configuring the target software) to create a baseline and snapshot it for that particular malware test. When your environment is ready, you can begin the dynamic analysis.

- Load the malware on the system, and start your monitoring applications. This process includes taking initial file and Registry snapshots using RegShot, as well as starting Wireshark, Process Monitor, Process Explorer, FakeNet and TCPView.

- Next, execute the malware and monitor its activities using the monitoring tools. When the malware activity quiets down, take a second snapshot with RegShot, stop all the other running tools (e.g., WireShark, Process Monitor and FakeNet), and terminate the malware executable.

- Finally, analyze the artifacts collected from the monitoring tools to further understand the malware. Based on your observations, you may need to
re-run the analysis with different parameters (waiting longer before stopping the analysis, executing malware in a different way, etc.). If this is the case, simply copy off the prior artifacts, revert back to your starting malware test snapshot, and rerun the test.

**Static Analysis.** Static analysis is by far the best way to understand the malware logically; however, it is also the hardest technique to learn and perform. It is easy to go from developers’ written code into machine-readable assembly instructions through compilation, but it’s very difficult to do the reverse. This is especially true if malware authors have performed any obfuscation techniques.

Tools like OllyDbg and IDA Pro help analysts reverse this process to gain a logical understanding of the malware, with the goal of creating readable code. Although performing a quick static analysis using indicators from the triage and dynamic analysis phases, doing a complete logical analysis is a fairly advanced topic and is beyond the scope of this article.

For those wanting to dig deeper into malware analysis, numerous free resources exist on the Web (see “Where to Go for More on Malware Analysis,” p. 29), but first, and most importantly, you need to practice. The best way to learn and improve your malware analysis skills is simply to perform the process again and again.

With practice comes proficiency, and with proficiency comes a stronger security posture for your organization. @

---

SALVADOR “GRECS” GREC is a United States-based (ISC)² member and frequent presenter on malware analysis. This article is based on his popular “Malware Analysis 101: From N00b to Ninja” presentation. For more of his articles and opinions, Salvador blogs at NovaInfosec.com and tweets at @grecs. When not writing, he is busy improving and architecting SOC and other security solutions.
# Malware Analysis Recommended Reading/References

We mentioned a lot of tools and resources in this article. Here's a rundown of all of them, with links to assist you in your own malware analysis learning.

## ONLINE AUTOMATED ANALYSIS
- **Malwr.com** [https://malwr.com/](https://malwr.com/)
- **Anubis** [http://anubis.iseclab.org/](http://anubis.iseclab.org/)

## WINDOWS SYSTEMS TO TEST ON
- **Modern IE** [http://www.modern.ie/](http://www.modern.ie/)

## TRIAGE ANALYSIS TOOLS
- **PeStudio** [http://winitor.com/](http://winitor.com/)
- **PE Explorer** [http://www.heaventools.com/overview.htm](http://www.heaventools.com/overview.htm)

## DYNAMIC ANALYSIS TOOLS
- **WireShark** [https://www.wireshark.org/](https://www.wireshark.org/)

## STATIC ANALYSIS TOOLS
- **OllyDbg** [http://www.ollydbg.de/](http://www.ollydbg.de/)
- **Malware analysis Linux distribution** created by Lenny Zeltser [http://REMenux.org](http://REMenux.org)
- **MALWARE SOURCES TO LEARN WITH**
  - **Practical Malware Analysis Labs** [http://practicalmalwareanalysis.com/labs/](http://practicalmalwareanalysis.com/labs/)
  - **Contagio** [http://contagiodump.blogspot.com/](http://contagiodump.blogspot.com/)
  - **VirusShare** [http://virusshare.com/](http://virusshare.com/)
  - **Malware Traffic Analysis** [http://malware-traffic-analysis.net](http://malware-traffic-analysis.net)
  - **Popular site for searching for malware hashes** [https://www.virustotal.com](https://www.virustotal.com)
  - **Two sites offer older versions of free and open source software that malware may be written for** [http://www.oldversion.com; http://www.oldapps.com](http://www.oldversion.com; http://www.oldapps.com)
- **OPENSECURITYTRAINING.INFO**
  - **“Intro x86”** [http://opensecuritytraining.info/IntroX86.html](http://opensecuritytraining.info/IntroX86.html)
  - **“Reverse Engineering”** [http://opensecuritytraining.info/IntroductionToReverseEngineering.html](http://opensecuritytraining.info/IntroductionToReverseEngineering.html)
  - **“Malware Dynamic Analysis”** [http://opensecuritytraining.info/MalwareDynamicAnalysis.html](http://opensecuritytraining.info/MalwareDynamicAnalysis.html)
- **ZELTSER.COM**
  - **Intro to Malware Analysis** [https://zeltser.com/?s=Introduction+to+malware+analysis](https://zeltser.com/?s=Introduction+to+malware+analysis)
BUILDING A BIGGER PIPELINE

THE 2015 (ISC)² GLOBAL WORKFORCE STUDY SHOWS WE MUST FUNNEL MORE PEOPLE INTO INFORMATION SECURITY...AND SOON

BY ANNE SAITA

NGELA MESSER WAS excited when she read the results of the 7th (ISC)² Global Information Security Workforce Study (GISWS), not by the growing shortage of qualified security professionals but by the call to action the findings portend.

“We all say we need more talent, but what we’re now finally focusing on is what to do to bend the demand,” she says.

“In the last several years, cyber has hinged on awareness, not just from the IT security staff but the CISO and CIO,” continues Messer, an executive vice president who leads the predictive intelligence business at Booz Allen Hamilton, an (ISC)² partner in the study. “The C-suite now gets it, so there is now more acknowledgement of just how important these skills are. This is a big step in showing we’re well on that path.”

A big step, perhaps, but what it may need are huge leaps.

This year’s GISWS is based on nearly 14,000 respondents globally, comprised of both (ISC)² members and non-members. The majority of respondents are located in North America (with a decent turnout from pros in Asia and Europe). A third of them hold management or executive positions, and two-thirds work at companies with 10,000 employees or more.

<table>
<thead>
<tr>
<th>Top 10 Security Concerns</th>
<th>(Selected as Top or High Concern)</th>
</tr>
</thead>
<tbody>
<tr>
<td>72% APPLICATION VULNERABILITIES</td>
<td></td>
</tr>
<tr>
<td>71% MALWARE</td>
<td></td>
</tr>
<tr>
<td>65% CONFIGURATION MISTAKES / OVERSIGHTS</td>
<td></td>
</tr>
<tr>
<td>60% MOBILE DEVICES</td>
<td></td>
</tr>
<tr>
<td>59% HACKERS</td>
<td></td>
</tr>
<tr>
<td>59% FAULTY NETWORK / SYSTEM CONFIGURATION</td>
<td></td>
</tr>
<tr>
<td>54% INTERNAL EMPLOYEES</td>
<td></td>
</tr>
<tr>
<td>49% CLOUD-BASED SERVICES</td>
<td></td>
</tr>
<tr>
<td>48% CYBER TERRORISM</td>
<td></td>
</tr>
<tr>
<td>42% TRUSTED THIRD-PARTIES</td>
<td></td>
</tr>
</tbody>
</table>
The most significant finding from the study is the growing gap in skilled labor at a time when transformative technologies like cloud services, software-defined data centers and the proliferation of mobile endpoints are taking over enterprises.

The workforce shortage has allowed those already in the field to command higher salaries, especially if they carry security-specific credentials, but those bigger paychecks come at a cost: higher demands on the workers. That may be why, despite the vast majority of respondents saying they like their current jobs, almost 20 percent sought new positions last year.

"Right now, there are 200,000 open infosec positions in this country that we can't fill," says Sumo Logic CISO Joan Pepin shortly after results were released in April.

That fulfillment problem may be due to too few companies offering entry-level positions and too many wanting only ideal candidates. "The attitudes of these hiring managers absolutely need to change," says Mark Aiello, president of Cyber 360, an HR placement firm focused 100 percent on cyber security and a study partner. "We keep hearing that there's a shortage of candidates, and I say, 'No. What there is is a shortage of perceived perfect candidates. There is not a shortage of candidates.'"

If those attitudes fail to change and emerging technologies continue their rapid adoption, the survey predicts that this workforce shortage could widen by 2019 to 1.5 million available positions.

"We are spending more money, but we are not getting any better at it—that's what our survey respondents are saying," Frank Dickson, research director for information and network security at Frost & Sullivan, told an audience at April's RSA Conference in San Francisco.

Part of that spending increase appears to be bigger salaries for those holding (ISC)² certifications. Worldwide, the average annual salary was US$97,778. Within that figure, however, (ISC)² members earn 35 percent more on average than their non-member counterparts—$103,117 vs. $76,363.

"I always say security certifications do matter, because you can make more money if you have one," Mark Aiello, president of the recruiting firm Cyber 360, says. "This study validates that."

**Summary**

- The study found a growing gap in skilled labor.
- Workforce shortage has allowed for higher salaries, but at a cost of increased demands.
- Fulfillment problem due to mismatch between supply and demand.
- Attitudes of hiring managers need to change.
- Survey predicts workforce shortage could widen by 2019.
- (ISC)² members earn 35% more than non-members on average.

**Top 10 Common Threat Techniques**

<table>
<thead>
<tr>
<th>Technique</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing (Social Engineering)</td>
<td>54%</td>
<td>37%</td>
<td>39%</td>
</tr>
<tr>
<td>Spambot</td>
<td>36%</td>
<td>32%</td>
<td>45%</td>
</tr>
<tr>
<td>Web Application Attacks (Other than SQL Injection)</td>
<td>35%</td>
<td>30%</td>
<td>35%</td>
</tr>
<tr>
<td>Privilege Abuse (Insider Misuse)</td>
<td>34%</td>
<td>29%</td>
<td>35%</td>
</tr>
<tr>
<td>Denial of Service and Distributed Denial of Service</td>
<td>33%</td>
<td>25%</td>
<td>27%</td>
</tr>
<tr>
<td>SQL Injection (Hacking)</td>
<td>31%</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Downloader (Malware)</td>
<td>29%</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>Command and Control (Malware)</td>
<td>27%</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Backdoor (Malware)</td>
<td>26%</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Spyware / Keylogger (Malware)</td>
<td>25%</td>
<td>20%</td>
<td>25%</td>
</tr>
</tbody>
</table>

**Where Increases in Information Security Are Projected**

**Security Tools**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>37%</td>
<td>32%</td>
<td>45%</td>
</tr>
</tbody>
</table>

**Personnel**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>34%</td>
<td>30%</td>
<td>35%</td>
</tr>
</tbody>
</table>

**Outsourced or Managed Services**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>28%</td>
<td>25%</td>
<td>30%</td>
</tr>
</tbody>
</table>

**Training and Education**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>33%</td>
<td>28%</td>
<td>31%</td>
</tr>
</tbody>
</table>

**Professional Services**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25%</td>
<td>22%</td>
<td>27%</td>
</tr>
</tbody>
</table>

**Certification**

<table>
<thead>
<tr>
<th>Year</th>
<th>2011</th>
<th>2013</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>28%</td>
<td>23%</td>
<td>26%</td>
</tr>
</tbody>
</table>
The study also revealed how companies are coping in the short-term with the gap in skilled labor: by essentially pushing security-related functions on other staff who have little to no information security experience. This “force multiplier” can cause slowdowns and other suboptimal results that cyber criminals are all too eager to exploit.

Part of the problem is that information security is a specialized field, requiring years of experience and high critical thinking skills. This is creating a shift in higher education, where curricula are being reconfigured based on current needs, and more scholarships are emerging to encourage students, particularly women and minorities, to consider information security as a college degree.

But the profession also requires practical experience, and companies have been slow to provide those opportunities.

“Something I hear over and over again is that we do have students graduating from schools, but there are no entry-level positions for them. I’d challenge organizations to build internships and entry-level positions so more people gain experience,” Elise Yacobellis, director of development, Americas Region for (ISC)², said during the RSA panel.

“If you do not put a stake in the ground now, we’re never going to see that growth,” she added.

‘IT TAKES A VILLAGE’ TO RAISE A CYBER WARRIOR

With television programs like CSI Cyber and Scorpion and action movies like Blackhat, Hollywood has helped update the image of cybersecurity workers from cellar-dwelling dweebs to the cool kids, but if we’re going to truly fill that pipeline with future cyber security warriors, we need to reach out to kids in childhood.

“It takes a village to solve the supply problem,” says Booz Allen Hamilton’s Messer. Experts like Messer believe recruitment should start no later than middle school, when students’ attitudes and aptitudes in science, technology, engineering and math begin to take shape. Games and hackathons can help locate raw talent, and scholarships can help fund both college and non-traditional career paths—such as cybersecurity grants for veterans in transition.

“I think our government needs to help with people’s education so that they can go to school without taking on a lot of debt,” Pepin says. “And we need to do something about the horrible technology gender gap, which has women leaving at a record rate.”

(ISC)² will release survey findings on women in information security this fall).
Higher education also needs to offer courses that meet the dynamic skills required for our current and future workforce. Programs such as (ISC)²’s Global Academic Program help bridge the knowledge gap through a joint framework with a growing network of colleges offering degrees in information security.

“We need to think outside the box to solve this problem,” Messer says. For instance, Booz Allen Hamilton has a Cyber SIM program within its internal “Cyber University” that takes a challenge-based approach to threat response. The training platform has proven so popular that the company’s clientele now want similar simulations to recruit, retain and retrain their own security staffs.

Cyber SIM, GAP and other initiatives are a start. But, as Frost & Sullivan’s Dickson and Michael Suby, VP of Research, write in a white paper, we have a long way to go and not a lot of time to get there:

“As a concerned and collaborative effort across organizations and disciplines, a security workforce that can address the evolving needs and complexities of cybersecurity and usher in safe and security cyber innovation is possible.

“This possibility; however, cannot wait. The time to act is clearly now.”

ANNE SAITA is editor-in-chief of InfoSecurity Professional.
THE FORCE BEHIND OUR BIENNIAL SURVEY

BY JULIE FRANZ

WE AT THE (ISC)² FOUNDATION have spent a lot of time in recent months talking about the results of the 2015 (ISC)² Global Information Security Workforce Study (GISWS), which shows a widening gap between growing demand for information security personnel and the pool of qualified applicants.

These national discussions, ranging from recruitment tactics to the rationale for a 20 percent job churn, are possible because almost 14,000 of you took the time to share your invaluable insights. This was not a quick exercise, and on behalf of everyone in our organization, I thank you for answering all those questions and encouraging your colleagues to do the same.

So what did we glean from the results? Many of you love what you do but are stressed by unmanageable workloads and emerging threats. You need more help, and even if your company has promised to expand its security operations, it may not be enough to keep pace with the rate at which enterprises are adopting new technologies. As a result, you’re pulling in people from elsewhere in IT to help reduce the risks of a compromise. Meanwhile, cybercriminals appear to be relying on your own workforce to aid in their illegal activities, given phishing is still the most effective means of breaching systems.

During a panel I moderated at this spring’s RSA Conference, Angela Messer of Booz Allen Hamilton said it takes a village to solve the supply problem. In other words, we need to devote more resources from many different organizations (government, private industry, education and non-profits like ours) to locate and train promising candidates, particularly those with non-traditional backgrounds.

It also took a village to produce this report. We started with Frank Dickson and Michael Suby at Frost & Sullivan to hone questions and accurately sort and display responses—no easy task, given the biennial GISWS is considered the industry’s most comprehensive report on the information security profession.

We also worked with partners Booz Allen Hamilton, NRI Secure Technologies and Cyber 360, and together we created a widely distributed white paper that outlines results and a call to action.

Some of those findings are detailed elsewhere in this magazine. Other results—particularly affecting women in security—will be showcased this fall in another white paper.

Many of you love what you do but are stressed by unmanageable workloads and emerging threats.

Finally, in addition to taking the time to complete the survey, many of you are (ISC)² Foundation donors, which means you contributed financially to fulfilling this enormous project. We are perhaps best known for our Safe and Secure Online program, which brings cybersecurity awareness to schools, and for providing undergraduate, graduate and faculty scholarships. But we also fund research such as the GISWS to raise awareness, start a global dialog and facilitate change.

We at the Foundation are grateful for the personal investment you have made in us so that we can pay it forward through scholarships, partnerships and studies that help move us forward as an industry, too. @
“ISACA CERTIFICATIONS ARE WORTH ACHIEVING. THEIR VALUE GOES FAR BEYOND PASSING AN EXAM.”

— KHAWAJA FAISAL JAVED, CISA, CRISC
MANAGER OPERATIONS & ICT PRODUCTS
LAHORE, PAKISTAN
ISACA MEMBER SINCE 2004

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

Register at www.isaca.org/2015exams-ISC2

ACCOMPLISH MORE

UPCOMING CERTIFICATION EXAMS

12 September 2015*
Final Registration Deadline: 24 July 2015
*CISA and CISM only. Held in select locations.

12 December 2015
Early Registration Deadline: 19 August 2015
Final Registration Deadline: 23 October 2015
Hurry—register early for a December exam to save US $50!

Register online for any exam to automatically save US $75! www.isaca.org/2015exams-ISC2
Minutes With...

GREG MAZZONE

Greg Mazzone is an information security consultant, providing security architecture analysis and advice within the Australian Federal Government security environment context. An (ISC)²® member since 2003, Greg claims Adelaide, Canberra and Melbourne as his hometowns.

EDITED BY ANNE SAITA

How did you get your first “big break” in information security?
My ‘big break’ was more of a ‘shattering.’ I had a rock climbing accident 20 years ago that resulted in a foot injury, which required me to shift career paths. My previous role was doing systems and process analysis and design in large manufacturing environments—which was just too much time on my foot. Faced with a disruptive life event, I took a leap and went back to university to earn a business and info sys degree. During this time, I purchased an MSDN subscription that gave me access to all of the Microsoft technologies, and I proceeded to do self-directed unstructured learning (play). At the end of my final year, a university lecturer invited me to an ISACA chapter meeting, and after a chance meeting with a partner of an IT Audit practice, I was offered a job. I wasn’t an overly popular IT auditor from the perspective of the financial auditors, as I often found security issues that had gone unnoticed/detected by the former IT auditors, and this increased the amount of substantive audit procedures the financial audit teams had to do. I soon realised there was a ‘gap’ in the industry for information security professionals that understood both business and information technologies. It was about then that I obtained my CISSP.

What did you want to do when you were 10 for a career? What happened afterward that that led you to your current position?
Astronaut and pilot—loved the idea of flying. A common route was via AirForce. Unfortunately, my need for prescription glasses blocked that route.

What is going on in the Land Down Under in terms of security issues?
What is keeping you up at night?
“Ah, she’ll be alright—it’s not like we have the same problems that they seem to have overseas.” This is something I have actually heard on many occasions—often from senior executives. There is the perception that we (in Australia) don’t have the same extent of cybersecurity issues (data breaches, etc.) as other countries do because there are so few media reports of them occurring in Australia. In Australia we do have some ‘light-touch’ laws on data breach notification that are arguably provider-biased rather than individual-centric, which advises ‘if a data breach creates a real risk of serious harm to the individual, the affected individuals should be notified’—noting that the assessment of this is made by the organisation responsible for the breach, and the requirement to notify is a ‘should’ only and is not compulsory.

Recently, I was contacted by my bank and informed that the debit credit card they had provided me was cancelled and would be replaced, as they had been informed by the credit card vendor that my data might have become comprised by a vendor. When I asked for information about who the vendor was, I was notified that they could not release that information for their privacy reasons (sic) to protect the vendor. Apparently, there was a big enough risk to the financial institutions to warrant the cost of re-issue, but I had no recourse to learn about a vendor who may have inadequate procedures to protect my data.

Greg Mazzone reveals more in our up-coming August 2015 e-newsletter, INSIGHTS.
ADVANCE YOUR BRAND WITH CUSTOM CONTENT
TWIRLING TIGER PRESS IS YOUR PUBLISHING SOLUTION

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

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

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

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

Contact us today at info@twirlingtigerpress.com.

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

www.twirlingtigerpress.com

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

PUBLICATIONS | WHITE PAPERS | SOCIAL MEDIA