NO BUDGET? NO PROBLEM!
14 LOW- OR NO-COST SECURITY SOLUTIONS

also
5 MINUTES WITH HUSIN JAZRI

MENTOR: IT’S GOOD FOR YOU WORKING TO IMPROVE THE FUTURE WORKFORCE

HOW TO HANDLE TEST ANXIETY
POWER YOUR CAREER
MASTER’S IN CYBER SECURITY OPERATIONS AND LEADERSHIP

Cyber crime is on the rise and today’s employers are looking for tech-savvy people to combat online criminals. Prepare yourself for these growing opportunities by earning your Master’s in Cyber Security in 20 months and join the fast and exciting world of Cyber Security.

- Top 100 nationally ranked university
- Curriculum dedicated exclusively to critical aspects of cyber security
- Immersive and unique career-building education
- 100% online: flexibility for busy professionals
- Complete the degree in 20 months

USD offers an on-campus Master of Science in Cyber Security Engineering

» (619) 260-4580 | (888) 832-0239
» CyberOps.SanDiego.edu
FEATURES

› TECHNOLOGY

14 No-Cost or Low-Cost Security Tools
Most of us need to be cost-conscious when it comes to adopting new security products. For those who are watching their budget dollars, an (ISC)²® member shows more than a dozen freeware or low-cost security tools that can dramatically improve your security posture. BY KEVIN GENNUSO

› MANAGEMENT

Guiding the Future
A successful mentoring program can improve your productivity and bench strength. BY JEFF SILVER

› PROFESSIONAL DEVELOPMENT

Sharpening Your Sword
There’s more than one way to help hopeful students become helpful information security professionals. BY RONALD WOERNER

› PERSONAL DEVELOPMENT

Don’t ‘Choke’
Whether it’s a crucial presentation or certification exam, you can conquer your anxiety. BY DEBORAH JOHNSON

Mentoring is a great way to elevate the caliber of information security professionals just entering the field. PAGE 18
Editor’s Note

GETTING BACK ON TRACK

IT’S MARCH, which means some of the personal and professional plans you devised in December are already falling apart. Maybe you didn’t budget enough resources, and as a result, you’re stressed, disappointed and discouraged.

This issue is all about solutions so that the hopefulness that peaked in January doesn’t turn to helplessness by July.

First up for those budget-conscious security professionals is a great list of free and low-cost solutions from Kevin Gennuso, an (ISC)² member who packed the room last fall during his presentation on a similar subject at Security Congress. His article includes tools not talked about at Congress and why they haven’t gotten the attention they deserve.

Jeff Silver, another (ISC)² member, also spoke at Congress and was inspired to create a piece on mentoring, which provides as many potential benefits to the mentor as it does to the protégé. Knowing someone is turning to you for career advice is a great way to raise your own skills and productivity because you want to set a good example. You also want to set expectations so that you truly assist someone just launching a career.

As someone who breaks out in hives at the mere mention of a “test,” I also found Deborah Johnson’s tips on alleviating test anxiety to be highly valuable. So, if your professional development plan includes new certification exams or just a plan to break out of your comfort zone with something way outside your wheelhouse, the article’s expert advice can help reduce stress and raise the likelihood of an excellent outcome.

As always, thanks to all who contribute to this and every issue through your ideas, submissions and critiques.

› ANNE SAITA asaita@isc2.org

ADVERTISER INDEX

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

University of San Diego ......................... 2
Capella University ................................ 5
InfoSecurity Europe .............................. 7
(ISC)² .................................................. 11
(ISC)² .................................................. 13
(ISC)² .................................................. 21
(ISC)² .................................................. 30
(ISC)² .................................................. 31
(ISC)² .................................................. 32
Twirling Tiger Press................................. 27

© Rob Andrew Photography

(ISC)² MANAGEMENT TEAM
SENIOR MANAGER, MEMBERSHIP MARKETING AND MEDIA SERVICES
Jessica Smith
727-785-0189 x4063
jsmith@isc2.org

EXECUTIVE PUBLISHER
Timothy Garon
508-529-6103
tgaron@isc2.org

MANAGER, GLOBAL COMMUNICATIONS
Amanda D’Alessandro
727-785-0189 x4021
adalessandro@isc2.org

MEDIA SERVICES COORDINATOR
Michelle Schweitz
727-785-0189 x4055
mschweitz@isc2.org

SALES TEAM
EVENTS SALES MANAGER
Jennifer Hunt
781-685-4667
jhunt@isc2.org

REGIONAL SALES MANAGER
Lisa O’Connell
781-460-2105
loconnell@isc2.org

EDITORIAL ADVISORY BOARD
Elise Yacobellis (ISC)²
Amanda D’Alessandro (ISC)²
Jawwad Malik EMEA
J.J. Thompson U.S.A.
Carlos Canoto South America
Dr. Meng-Chow Kang Asia

TWIRLING TIGER PRESS INC.
EDITORIAL TEAM
EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

PROOFREADER
Ken Krause

INFOSECURITY PROFESSIONAL
© Twirling Tiger Press Inc.
www.twirlingtigerpress.com

This partnership reflects (ISC)²’s commitment to supplier diversity.

© Rob Andrew Photography

T"
HEALTH CARE SECURITY JOBS HAVE TRIPPLED SINCE 2007*

*SOURCE: Labor Insight Jobs (Burning Glass Technologies)

ARE YOUR SKILLS UP TO MEETING THE CYBERSECURITY CHALLENGE?

Up-to-date security skills gained with Capella’s Master’s in Health Care Security can help you meet the needs of this important and fast-growing field.

Why choose Capella?

• You’ll gain practical, hands-on experience working with industry-specific tools, helping you develop the cybersecurity expertise health care employers require.

• Our program aligns with the NSA Health Care Security focus area, which will earn you a digital badge to validate your mastery of health care security.

• Already have your CISSP®? You could be 40% of the way to your degree, saving you time and money.

MEET THE DEMAND. START TODAY. Capella.edu/ISC2 or 1.866.933.5836

ACCREDITATION: Capella University is accredited by the Higher Learning Commission.
HIGHER LEARNING COMMISSION: https://www.hlc.org; 800.221.7681
CAPPELLA UNIVERSITY: Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis MN 55402; 1.888.CAPPELLA (227.3552) 16-8546
After more than 30 years of working with publicly traded and nonprofit companies, I understand the confusion that surrounds the terms “not-for-profit” and “tax-exempt.” Contrary to popular belief, just because (ISC)² is a nonprofit tax-exempt corporation does not mean it cannot generate a surplus. Rather, these surpluses are important so that we may funnel funds back into our member programs and remain a healthy, professional organization that will continue to certify and educate cyber, information, software and infrastructure security professionals for years to come. Continued financial investment is important to meeting our mission and vision as our international membership grows.

Members who want to know more about our financial health can review our annual report (https://www.isc2.org/management-annual-reports/default.aspx), which includes our annual independent audit results. The annual financial results presented each year reflect the company’s working capital and financial position.

Whether we’re an organization of 150, 150,000 or 150 million members, it’s good business to have a healthy cash flow to funnel back into the organization. Our organization directs our excess cash flow into our membership through the development and maintenance of our professional programs and member benefits.

The (ISC)² focus on the cyber, information, software and infrastructure security professions is what distinguishes us from other organizations. The (ISC)² focus on the cyber, information, software and infrastructure security professions is what distinguishes us from other organizations. Our certification programs are often the draw to join our membership, but it’s the value-added products and services we then provide to members that help aid or even accelerate their career advancements.

I’m proud to be part of a strong team at (ISC)² that is dedicated to helping each and every member succeed so that together, we help make the cyber world a safer place.
Everyone and everything you need to know in security

Rather than taking our word for it, look at the facts below:

- **98%** satisfied visitors at Infosecurity Europe 2015
- **93%** satisfied exhibitors with 80% rebooking at the exhibition
- **160 hrs** of free seminars and workshops
- **315+** vendors and service suppliers delivered a diverse range of new products and services
- **ROI £1.39+ bn** of estimated future orders, visitors expect to place with exhibitors as a result of attending Infosecurity Europe
- **4,435** professionals earned CPD / CPE credits

REGISTER YOUR INTEREST

http://www.infosecurityeurope.com
(ISC)² TO SPONSOR ISO/IEC/JTC1/SC27 2016 MEETINGS

(ISC)² is pleased to sponsor the April 2016 Plenary and Working Group meetings of ISO/IEC/JTC1/SC 27 in Tampa, Fla. More than 300 international experts will come together to assess the efficacy of the international standards in helping organizations protect their information.

Since 2011, (ISC)² has supported ISO activities, first as Category C, and soon thereafter as Category A Liaison to the JTC1/SC 27 working groups.

In a letter, JTC 1/SC 27 Secretariat Krystyna Passia expressed the group's appreciation for (ISC)²'s sponsorship, saying: “We believe that the hosting of the SC 27 meetings by (ISC)² in Tampa will be a very successful and productive event. Once again, we wish to express our warmest thanks to (ISC)².”

(ISC)²’s CEO David Shearer, in a letter to SC 27 members, commended the group’s work, commenting, “SC 27 plays a prominent role in progressing critical international standards and is at the helm of expertise on information and IT security standardization. As a liaison organization, (ISC)² is privileged to work with voting countries, observing countries and other liaison organizations that contribute to the work of SC 27.”

(ISC)² also would like to congratulate SC 27 on receiving the Lawrence D. Eicher Award for 2015. The award is given each year to the ISO technical committee or subcommittee that has distinguished itself in making significant contributions to the development of International Standards.


“As a liaison organization, (ISC)² is privileged to work with voting countries, observing countries and other liaison organizations that contribute to the work of SC 27.”

—DAVID SHEARER, CEO, (ISC)²

LET YOUR CREDENTIALS STAND OUT

(ISC)² members will soon have a new way to communicate their accomplishments. It’s a digital badge that represents their certification(s), and it can be attached to email signatures and social media profiles. Each of seven badges is “clickable” so a person can see what skills and practical requirements the holder achieved to earn the badge.

The digital badges are possible through a partnership with Acclaim, a platform of Pearson VUE, the world’s leading learning company. Acclaim and (ISC)² strictly control the integrity of the badges to ensure that only those who have earned a certification can claim the associated badge.

(ISC)² encourages members to use digital badges to promote their own skills by visiting the (ISC)² website for downloads.

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 you two Group A CPEs.

(ISC)² NAMES NEW DIRECTOR OF PROFESSIONAL PROGRAMS DEVELOPMENT

(ISC)² has named Dr. Casey Marks, former chief executive officer at Cambridge Michigan Language Assessments, as the new (ISC)² director of professional programs development. He has more than 20 years of experience in large-scale assessment and has published and presented extensively.

He is recognized as an expert on issues related to adoption and vendor transition of computer-based testing for high-stakes, large-scale testing programs, international program expansion and examination security. Marks has a long history of involvement and volunteer service with testing-related organizations, such as the American Education Research Association (AERA), American National Standards Institute (ANSI) and many others.

As the director of professional programs development, he serves as the lead executive developing psychometrically sound and legally defensible professional certifications that advance the mission and vision of (ISC)². (ISC)² CEO David Shearer said, “Casey was highly recommended for this position by respected industry professionals. He’s an accomplished psychometrician with COO- and CEO-level business experience, which made him an ideal fit for the director of professional programs position. I am confident that he will do great work for the organization, and I feel very fortunate to have him on our team.”

Marks called (ISC)² the IT industry standard for cyber, information, software and infrastructure security certifications.

“It is an honor and a privilege to be part of an organization that is helping shape the future of our society,” he said. “With the rapid advancement of technology in all aspects of our lives, I am cognizant, more than ever, of the need to make a safe and secure cyber world. I look forward to bringing my expertise in assessment and credentialing to help (ISC)² realize that vision.”

“Dr. Casey Marks called (ISC)² the IT industry standard for cyber, information, software and infrastructure security certifications. (“He’s an accomplished psychometrician with COO- and CEO-level business experience, which made him an ideal fit for the director of professional programs position.” —David Shearer, CEO, (ISC)²)

US$75.4 BILLION
Amount in 2015 spent on information security, up 4.7% from the previous year.


64% of consumers surveyed worldwide are unlikely to shop or do business again with a company that had experienced a breach where financial information was stolen.

Source: Gemalto (Meudon, France) 2015 survey of 5,750 consumers in Australia, Brazil, France, Germany, Japan, United Kingdom and United States
**FIELD NOTES**

**SPOTLIGHT: (ISC)²® NEW YORK METRO AND QUANTICO CHAPTERS**

**(ISC)² CHAPERS PAY IT FORWARD**

As (ISC)² chapters around the globe work to advance information security in their local communities, their members gain valuable experience through professional development, networking, education and training. They are also able to impact the next generation of cybersecurity professionals directly through volunteering their time to lead events and fundraise. Those efforts have enabled some chapters to make scholarship donations to the (ISC)² Foundation, which is changing its name this year to the Center for Cyber Safety and Education.

The (ISC)² New York Metro Chapter was able to do just that. Chapter president and current Columbia University student Nancy Collins recognized the need. “Understanding fully the challenges of paying for an education provoked me to find a way where my chapter can contribute to this cause.”

With its recent donation of US$1,300 to the Center’s Undergraduate Scholarship Program, the New York Metro Chapter is helping smooth the way for the future information security practitioners.

The Quantico Chapter in Virginia also recently contributed US$1,000 to the scholarship program, the first year the chapter has been able to do so.

The Quantico Chapter is looking forward to supporting the nonprofit’s ongoing efforts to advance the education of information security majors enrolled in universities worldwide. As the chapter continues to grow, it will seek to develop its own scholarship program geared toward local high school students to support the (ISC)² goal of developing regional young professionals attracted to information security.

The need is great, given last year’s much-publicized Global Information Security Workforce Study (https://www.isc2cares.org/IndustryResearch/GISWS/), which revealed a shortfall of 1.5 million cybersecurity professionals over the next five years. The future of information security lies with the students pursuing these degree programs today. As the New York Metro and Quantico Chapters have proven, raising scholarship funds for deserving students is a worthwhile investment in the profession’s future.

**CHAPTER CONTACT INFORMATION**

**NEW YORK METRO**

President: Nancy Collins  
Email: ncollins@isc2chapter-nymetro.org  
Website: https://www.isc2chapter-nymetro.org/

**QUANTICO**

President: Doug Arntt  
Email: president@isc2quanticochapter.org  
Website: http://www.isc2quanticochapter.org

**LAST YEAR, CHIEF AND KEY EXECUTIVES GLOBALLY REPORTED**

- **69%** now use cloud-based cybersecurity services
- **54%** have a CISO in charge of the security program
- **38%** more security incidents were detected in 2015 than in 2014

Source: PwC: The Global State of Information Security® Survey (FY) 2016 based on responses from more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices in more than 127 countries.

**AREAS FINANCIAL SERVICE COMPANIES ARE MOST LIKELY TO BE ’VISUALLY HACKED’**

- Lobbies and public areas
- Teller desks
- Platform desks
- Printers, copiers and fax machines
- Drive-up teller windows
- Shared/open workstations

Source: Ponemon Institute’s 2015 Visual Hacking Experiment, sponsored by 3M Company and the Visual Privacy Advisory Council
(ISC)² Security Congress conferences make a global impact by advancing security leaders at each event through the multi-track educational sessions along with prime networking and career advancement opportunities. Each Security Congress will include topics on best practices, current and emerging issues, and solutions to challenges.

SECURITY CONGRESS
12-15 September 2016
Orlando, FL • Orange County Conv. Center
congress.isc2.org • #ISC2congress

SECURITY CONGRESS APAC
26-27 July 2016
Bangkok, Thailand
apaccongress.isc2.org • #ISC2congressAPAC

SECURITY CONGRESS EMEA
18-19 October 2016
Dublin, Ireland • Croke Park Stadium
emeacongress.isc2.org • #ISC2congressEMEA
12 Steps to Finding Malicious Activity Within Your Infrastructure

BY KASHIF IQBAL

ONE OF THE biggest challenges a security analyst faces is identifying and detecting potential malicious activities. I remember that when I started detecting potential malicious behavior within my organization roughly seven years ago, I found little information on the best way to sift and sort all those event logs without buying expensive solutions.

So I picked a SIEM solution and started importing every possible log I could think of, ranging from firewall and domain controllers to proxy, AV and Exchange services. Once I had all the data, the real hunt began to find the needle in the haystack.

I attended several security conferences and asked a lot of people, “So, how do you detect abnormalities in your logs?” I always received a huge variety of answers, from very expensive products to ingenious ways of using a SIEM solution. I started recording every method I came across in a diary, and I decided I should share my findings with my fellow (ISC)² members.

The key points listed have really helped me gain visibility into the network and detect anomalous behaviors. Is the list comprehensive? Hardly. But this is definitely a good place to start to flag suspicious activity that sets off an incident response.

1. **Monitor entry points into the network.** Since we all love to work from home these days, one of the key entry points into the network in every organization has become a remote access VPN. Therefore, you should monitor:
   - Passed and failed VPN accounts and map them against geographical locations.
   - Any geographical location change for a successful user’s login (e.g., a user login from the U.S.A. at 8 in the morning and again from Russia at 8:30 a.m. the same day).
   - How many users are logging on to a VPN and how long they remain connected.

2. **Look for mismatched ports with protocols.** For instance, identify any non-SSH application using port 22 or port 3389 that isn’t an RDP application.

3. **Consider how many successful and unsuccessful Active Directory logins are happening in working and non-working hours.** And, are there any unsuccessful login attempts triggering an unknown username or a username that doesn’t exist? When we initially put up this dashboard, it assisted our helpdesk a lot.

4. **Examine what types of file extensions are traversing through your network, such as PDF, ZIP, RAR and...**
many more. You can also correlate the file type with the file size.

5. See if you can pick any suspicious file names, such as g.exe, m.bat and p.js, where there is no legitimate use of these types of files.

6. Keep an eye on your Windows registry or manual registry keys creation.

7. Baseline your DNS requests, and keep an eye on too many DNS requests from any specific IP address or machine. You can also look for DNS requests host machines are making in regular intervals that might be beaconing the host.

8. Look in the web proxy to monitor parked domains and unknown categories of URLs. Also, look for any machine trying to access those domain names.

9. Scrutinize RDP sessions made outside of office hours. If you pick an RDP session on Sunday at 5 in the morning, it may signal malicious activity, since all the tech guys presumably are sleeping in after a fun and exhaustive Saturday night.

10. Monitor for abnormal amounts of traffic to malicious domains. You can import feeds and use lookups or watch lists for this.

11. Determine uncommon ports opened on the systems, which may indicate a new application and also some potential zero-day attacks.

12. Look at more than baseline event logs over the last couple of days to see if there’s any pattern in events. Be sure to compare your daily firewall logs to compare alerts against the baseline.

As I already mentioned, this is not an exhaustive list, but it does cover the basics. I am still learning new ways to identify abnormalities in today's continuously evolving landscape. Just keep asking yourself, “Do I have this level of visibility in my infrastructure to correlate with the intrusion kill chain?” If not, it’s time to get started.
CYBERSECURITY is a Really Big Deal for most companies nowadays, and the vendors who make security products are well aware of this. Just look at the increasing sprawl of the vendor exhibit floor at conferences like RSA and Black Hat. Seems like everyone has a new, shiny, expensive box that will protect you from the latest zero-days, APTs, ABCs or whatever newly coined buzzword they’re using.

But as anyone who has worked in this industry long enough knows, no matter how many times vendors claim to have a silver bullet, they don’t. And as much as we’d all like to purchase every new product, upgrade or add-on, very few of us have unlimited budgets—if we have security budgets at all.

THESE LOW-AND NO-COST SOLUTIONS CAN DRAMATICALLY IMPROVE YOUR SECURITY POSTURE

BY KEVIN GENNUSO

WANT TO HEAR MORE?
Listen to the 2015 (ISC)² Security Congress presentation that inspired this article. http://ow.ly/Xz1sG

PHOTOGRAPH BY CHANDLER CROWELL
But what if there were alternatives? What if there were low-cost, even free, solutions that can make dramatic improvements in an organization’s security posture?

Well, there are.

The people who make these products do so to improve their own lives and the overall community. Unfortunately, they don’t have massive marketing budgets or an army of sales critters, so these solutions sometimes get lost in the noise. Couple that with the stigma that is sometimes attached to free software, and no wonder they’re hard to find. CISOs are inundated with vendor pitches, sponsored after-parties and cold calls, all of which can help perpetuate the perception that “if it works so well, why aren’t they charging for it?”

We’ll explore a number of free and low-cost solutions that can significantly enhance any cybersecurity program. These tools and solutions fall into the following categories and can sometimes span across multiple domains:

- Access control
- Detection
- Forensics
- Logging
- Mitigation
- Prevention
- Security testing

1. MICROSOFT LAPS
   DOMAIN: ACCESS CONTROL

Yes, Microsoft has a freebie. They don’t talk about this tool very much, probably because they don’t charge anything for it. LAPS stands for Local Administrator Password Solution, and the name says it all. This is the fix for the local administrator problem, wherein local administrator passwords are difficult to change with any regularity and are often common across systems that have been built from a preconfigured image.

LAPS allows an organization to regularly change the local admin passwords of any system joined to the domain. The security team can then store those credentials in the Active Directory for future retrieval by the authorized admins. Admins can change passwords automatically at a preconfigured interval using whatever age, complexity, etc., is appropriate.

The local admin problem exists for any organization that uses Windows computers, so this tool is a welcome one and supplants many other commercial solutions that perform a similar task.

2. MICROSOFT EMET
   DOMAIN: MITIGATION

What’s that, you say? Another free tool from the house that Gates built? EMET stands for Enhanced Mitigation Experience Toolkit, and this one is very powerful.

EMET protects vulnerable software using “mitigations,” classes of protection mechanisms that defeat commonly used attack vectors. EMET is the fix for the Java problem—you know, the one where you have to keep old, bug-ridden versions of Java installed for some legacy application that requires it. It also fixes the Adobe Flash problem, which is the one where you need to install highly vulnerable software on your endpoints so that content-rich (read: pretty) websites paint correctly.

EMET is possibly the most powerful tool on this list, and professional penetration testers like David Kennedy recommend it because it makes his job difficult. It is free, and Microsoft fully supports it. It has its drawbacks, such as centralized logging, and it requires extensive testing before you can deploy it, but the benefits far outweigh the drawbacks.

3. EL JEFE
   DOMAIN: DETECTION

This solution helps blue teamers and incident responders identify potential threats in the environments they’re defending. The system includes a central Linux-based server and the Windows endpoints running the El Jefe client. The clients take an inventory of all binaries on the system and report them up to the server. They also keep an execution log of all binaries on the system, which is great for forensic investigations.

The system allows a defender to do things like search for unique binaries, parent/child process relationships and highly entropic binaries. A lot of these could indicate the presence of malware. El Jefe also tracks any USB devices that have connected to managed systems, which is helpful for tracking USB-borne infections.

4. SLEUTH KIT AND AUTOPSY
   DOMAIN: FORENSICS

These tools are the components of an excellent and free open source digital forensics toolkit. You can use them together to review a forensic image of a given system. It supports nearly all modern file systems, as well as Android devices. It can analyze disk images, local drives or individual files or folders.
Given the cost of commercial digital forensics tools, Sleuth Kit and Autopsy are a huge help to any team on a small budget requiring this capability.

Some of the features include keyword searching, deleted file recovery, registry analysis, Internet artifact analysis (think web history and email) and EXIF metadata extraction from image files. Modern versions run on Windows, but the 2.x versions are still downloadable and run on Linux. Given the cost of commercial digital forensics tools, Sleuth Kit and Autopsy are a huge help to any team on a small budget requiring this capability.

5. **GRSECURITY**  
**DOMAIN: MITIGATION**

Similar to (and possibly the father of) Microsoft EMET, grsecurity focuses on protecting the Linux kernel from zero-day attacks. It has been in active development for more than 14 years and provides numerous mitigations not available in other hardening technologies, such as SELinux. Upon install, it hardens the userland environment and chroot jails and randomizes memory and kernel structures to make an adversary’s shellcode much more difficult to execute.

Up until this year, this tool was free; however, due to numerous copyright violations by unnamed entities, the authors now require a donation in exchange for stable patch releases.

6. **MODSECURITY**  
**DOMAINS: MITIGATION, PREVENTION**

Challenged by an increased focus on patching and hardening operating systems, adversaries have turned to attacking web applications as a way to compromise networks. Trustwave’s ModSecurity is a free and open source web application firewall that prevents attacks against vulnerable web apps. It runs on the most popular web servers, including Apache, IIS and Nginx, and comes pre-loaded with the OWASP ruleset, which defends against the common vulnerabilities the OWASP Top Ten outlines (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

ModSecurity can also perform real-time blacklist lookups to drop traffic from known malicious hosts. Defenders can also tailor customer rules to the applications being protected. Trustwave also offers a commercial ruleset that provides malware, webshell and botnet detection, as well as “virtual patches” for common web apps, such as SharePoint, WordPress and Drupal.

7. **PFSENSE**  
**DOMAINS: ACCESS CONTROL, DETECTION, PREVENTION**

Look around at the “next-gen firewall” landscape, and you’ll find some feature-rich firewalls that do some pretty amazing things. That “next-gen” label, however, tends to come with a hefty price tag. pfSense is a free, open source firewall that you can outfit with many of the same features as a commercial next-gen firewall. It will run on most any hardware, and it has high availability features, OS-based rulesets and a highly customizable state table. And thanks to the slick packaging system, add-ons are a breeze. Need an IPS install for the Snort package? Are there certain categories of sites that aren’t allowed in your environment? Install the Squid Proxy package. There are hundreds of other packages to choose from, which might make pfSense the most next-gen of all the next-gen firewalls around.

8. **SECURITY ONION**  
**DOMAINS: DETECTION, LOGGING**

Open source, network-based intrusion detection systems can be daunting to deploy, and commercial systems can be out of reach for many security budgets. Security Onion is a free Linux distribution that focuses on intrusion detection. It incorporates multiple IDS engines, packet analyzers and log management. Setup is straightforward, and detailed videos and documentation are available. It also has a distributed architecture, allowing you to deploy multiple devices across as many network areas as you need to for full coverage.

There is an active user community supporting Security Onion as well, and they can answer most any question. It’s a great alternative to commercial products, and an even better alternative to having no idea if your network is under attack.

9. **ARTILLERY**  
**DOMAINS: DETECTION, PREVENTION**

The goal of this nascent tool is to detect potential attacks before they happen. It does this by opening TCP ports that aren’t actually used by the system it protects. If something connects to those honeypot ports, it assumes that the source is malicious and automatically blocks it. It also has the ability to pull lists of known bad IP addresses and add...
them to the block list. It supports both Windows and Linux and is both free and open source.

10. OPENNAC

**DOMAINS: ACCESS CONTROL, DETECTION, MITIGATION**

If you're familiar with the Center for Internet Security's Critical Security Controls (http://www.cisecurity.org/critical-controls.cfm) (and if you're not, you should be), the very first control on the list is having an inventory of authorized and unauthorized devices. Once you've established that inventory, defenders need a way to enforce it. Enter OpenNAC, a free network access control solution that allows for the detection and mitigation of unauthorized systems.

It can perform automatic endpoint discovery, allowing you to build that initial inventory. It also has support for multiple network hardware vendors. OpenNAC can use either 802.1x or a MAC address for authentication and can detect the operating system, anti-virus status and patch level of all endpoints.

It uses either SNMP or command-line access to detect endpoints and move them to the appropriate VLAN based on the endpoint’s trustworthiness. You can compile it from source executed from binaries or stand it up as a virtual appliance. There is also an enterprise edition that has full product support.

11. OSSIM

**DOMAINS: DETECTION, LOGGING**

Security incident event management (SIEM) products can be extremely expensive to implement properly due to the sheer capacity they require to process security events. The typical vendor response is, “Well, just buy more,” which isn’t surprising. Luckily, there’s OSSIM by AlientVault. OSSIM is a free, open source SIEM that has all of the features we typically see in a commercial SIEM, including event collection, normalization and correlation. It uses AlienVault’s Open Threat Exchange to help determine if traffic is malicious. Additional features are available in Unified Security Management, the commercial version of this product.

12. OSSEC

**DOMAINS: DETECTION/PREVENTION**

OSSEC is a free, open source, host-based intrusion detection system (HIDS) that provides a number of services, including log monitoring and forwarding, file integrity monitoring (FIM), rootkit detection, and alerting and response to problems it detects. OSSEC agents all report back to an OSSEC server, allowing for centralized collection and policy distribution. It works across nearly all modern operating systems, and Trend Micro fully supports it. The authors also highlight its strengths in meeting PCI-DSS compliance, which may be interesting to those who deal with payment cards.

13. OPENVAS

**DOMAIN: SECURITY TESTING**

OpenVAS is an open source vulnerability scanner and manager consisting of a few different tools wrapped into a single package. It was forked from Nessus in 2005 after Tenable decided to take the licence closed source. It is able to detect more than 35,000 different vulnerabilities that are categorized by type and severity.

Just like the commercial scanners, it can track vulnerabilities over time, and it can generate reports or output them to XML. It also has a scheduling feature, allowing you to schedule regular authenticated or unauthenticated scans. Users can also create their own network vulnerability tests if necessary. OpenVAS is free, but you can purchase training and an appliance from the creators.

14. OWASP ZAP

**DOMAIN: SECURITY TESTING**

ZAP stands for Zed Attack Proxy, and it’s an active OWASP project. ZAP allows for automated and manual security testing of web applications by giving the tester the ability to see and make changes to the raw traffic that passes between the client web browser and the web server. It has a spidering function for crawling websites, including an AJAX spider for sites that one cannot crawl using traditional methods. It has an active and a passive vulnerability scanner, multiple fuzzing engines, and parameter tampering and analysis features. It’s useful for anyone, from beginners to experts. Best of all, it’s free.

As you can see, there are some really powerful tools out there that just don’t get a lot of attention or space on the vendor floor at our industry’s conferences. This is just a small collection of the many free or low-cost security solutions available. With some additional research on these tools and others, you can see if they can address gaps in your information security program.

---

KEVIN GENNUSO, CISSP-ISSAP, is a Pittsburgh-based senior security information architect for Dick’s Sporting Goods.
A SUCCESSFUL MENTORING PROGRAM CAN IMPROVE A COMPANY’S BENCH STRENGTH

BY JEFF SILVER

HEN ONE conjures up images of mentoring, they’re often of a wise, bearded oracle late in his years imparting his lifelong wisdom to a youngster about to go off and start his adult life. While that might have been a scene from an old movie, it is not exactly how it works in the real world.

Today’s effective mentors have a wide diversity of age, experience and personality types within the industry. Not everybody is the right fit to be a mentor, but most security practitioners who have been in the industry long enough have a tremendous amount to offer. The key is establishing a program that empowers mentors, providing them with guidelines and training for effectiveness.
REWARDS FOR ALL
A successful mentoring program not only helps mentees with their career aspirations but has a positive impact on a company’s culture as well. Security professionals who have experienced successful mentoring have an increasingly positive view of their team and company, and they likely will want to remain at the company. The state of today’s job market for qualified technical professionals alone makes establishing a strong mentoring program an attractive project for any organization.

ESTABLISHING THE COMMITMENT
The mentoring relationship should last six months to one year, but no longer. The mentor should have enough time to make a positive impact, but not so much that things drag on to the point where the relationship languishes and becomes nonproductive. Six months gives the mentor enough time to cover key topics and allows for two distinct mentors per year, which can provide multiple perspectives on key development topics.

‘NICE TO MEET YOU’
One of the first goals for a mentor is to establish a trust relationship with his or her mentee. This is absolutely essential. It is always best to meet in person, but a remote meeting via video conferencing or Skype can work, helping to create a better conversational bond in spite of the geographical distance.

On the introductory phone call, let the mentee, sometimes also referred to as a protégé, know that you are looking forward to the relationship and what they can expect in the first scheduled meeting.

That first meeting will include sharing a bit about each other. This could be the first obstacle, but it’s a hurdle that must be overcome for the relationship to work right. Sometimes getting personal can be difficult, and (please excuse the stereotype!) it can be even more difficult for technical people.

On that initial scheduled meeting, mentors should always go first and share about themselves. Yes, you need to get personal. This is an opportunity for you to talk about how you got to where you are and what is important to you—not to brag, but to be genuine with your mentee. Share your successes, and, yes, any key failures that helped make you who you are today. It is important that the mentee sees that, like everyone else, you have had your share of challenges and the self-confidence to talk about them.

This will not only open the door for the mentee to feel comfortable enough to share about him/herself, but it will also allow for trust to take root.

The importance of this first step cannot be overstated. If a potential mentor is not willing to get personal up front, they may not be suited to be a mentor at all. Remember, just because your Tier III Forensics Analyst is the top technical guy in the organization, it does not necessarily mean that he is the right person to build up other security professionals.

IN THE BEGINNING
A biweekly meeting schedule is ideal, whether it will happen remotely or face-to-face.

Once you have initiated trust with the mentee, “brand building” is next. Now, you listen to the mentee’s current situation as a security professional and his or her career aspirations. Then, begin the process of helping that person take concrete actions to start achieving those goals.

Small homework assignments help achieve this and help stretch the security professional that you are guiding.

DISCUSSION POINTS
Include in the discussion a core set of exploratory topics based on what your protégé initially shares with you regarding career aspirations:

• Professional security organizations [(ISC)², Infragard, ASIS International, HTCIA, etc.]
• Certifications [Security+, CISSP, CEH, etc.]
• Reading rhythm [SC Magazine, books, blogs, etc.]
• Exotics

“What are exotics?” you ask. Exotics are any aspect of the job function that is not part of core duties. It is the “above and beyond.” There is no other area in which a security engineer professional builds his/her “brand” more strongly.

The world of professional “brand building” is a key area a strong mentor can really help develop. If you were to take a moment and reflect upon the most successful people you know in your field, they are typically men and women who have stretched themselves well beyond the boundaries of their traditional roles.

This discussion is crucial to brand building because it establishes your knowledge, abilities and willingness to help others inside and outside the company. Examples of exotics for the security engineer include:

• Writing field documentation for the broader company team
• Teaching to the internal technical team
• Speaking at a professional security organization
chapter meeting such as (ISC)² or Infragard
• Speaking at a larger industry event (e.g., annual conference)
• Creating internal training videos
• Performing competitive/comparative analysis of similar security products
• Building and maintaining a “product lab”

The idea here is to promote a creative thought process you and your mentee can explore together. It may take multiple sessions—up to two months—to cover this area, and it’s important that the conversation be both constructive and forward-moving. Once you feel that these topics have been covered, you can move on to other key areas of discussion.

STAYING FOCUSED
Your bi-weekly calls (or meetings) should stay on track. One of the hazards mentors may face is getting derailed by the mentee’s desire to share a current “tactical” issue they are dealing with that week. As the mentor, you must be time-aware, and if the issue is complex and time-consuming, let the mentee know that you want to give it the attention it deserves and will schedule a separate appointment to discuss it.

This disciplines your biweekly call to cover the key strategic discussion points you need to explore with your mentee without dismissing what very well may be an operational issue they are facing right now and want guidance on.

DIVING BELOW THE SURFACE
Corporate relationships are the next key topic, and this requires an adequate time investment. Begin with the mentee’s relationship with his or her boss since it’s the most important relationship. A mentor can truly help develop this relationship through thought-provoking questions for mentees that foster a productive relationship with their managers.

Key questions include:
• How often do you speak with your boss?
• How often do you meet face-to-face?
• One a scale of 1 to 10, how would you rate your relationship?
• What do you have in common with your boss?

A homework assignment can gauge how serious your mentee is about personal growth. A constructive and revealing question might be, “The next time we get together for our biweekly meeting, I would like you to tell me two new things you have learned about your manager.”

Exploring the topic of an immediate work group or team is also important, especially if the mentee is fairly new and trying to fit into an existing team of security professionals. A confidential conversation with the mentee’s manager will help you gain insight into and assess the “self-awareness” of your mentee. It is not uncommon, especially among technical people, to see a lack of self-awareness or blind spots in someone. A mentor can uncover these and gently guide a mentee toward greater awareness.

The kinds of questions that can elicit this information include:
• Tell me about the dynamics of your team.
• Who do you feel “tightest” with on your team?
• Who is the biggest complainer on your team?
• Who is the newest member of your team?
• On a scale of 1 to 10, what would you say your team cohesiveness level is?

FINDING CLOSURE
Nearing the six-month mark, it is important to make sure your mentee is prepared for the close of the mentorship. Although the friendship does not have to end, it is important to have a formal end to the mentoring relationship.

If you developed a strong connection with your mentee, there is certainly nothing wrong with checking in with him/her from time to time, but now it will be as a friend and a bit more informal.

EVERYONE CAN USE A MENTOR
Finally, remember, as a mentor, you also need to have “go-to” people in your life. Sometimes, situations are very complex, and the career of a young security professional may rest in some of your decisions and guidance. That is a sobering reality and one any mentor takes seriously.

When difficult or complex situations arise, the mentor may need the guidance and support of his/her own adviser, just as the mentor provides a sounding board to a (usually) less-experienced colleague. Mentors need not go it alone.

JEFF SILVER, CISSP, has been in the network security industry for more than 20 years, is an SE manager at RSA and an officer of the (ISC)² Delaware Chapter.
May 19th and 20th, 2016 | Washington DC
Walter E. Washington Convention Center

INSPIRING CHANGE AGENTS
in an Environment of Game Changing Threats

Keynote Speaker - Dr. Jennifer Golbeck
The University of Maryland's Director of the Human-Computer Interaction Lab, Jennifer Golbeck, will open Day 1 of CyberSecureGov addressing, “The Human Side of Cybersecurity.”

Keynote Speaker - Dr. David A. Bray
Harvard Visiting Executive In-Residence, Eisenhower Fellow, and CIO for the Federal Communications Commission, Dr. David A. Bray, will open Day 2 of CyberSecureGov addressing, “Positive #ChangeAgents in our Exponential Era”

Register Now » http://cybersecuregov.isc2.org
THE MANY WAYS WE CAN ALL BUILD TOMORROW’S INFORMATION SECURITY PROFESSIONALS—TODAY

BY RONALD WOERNER

YOU CHOSE well when you entered the information security career field. Your talents are in high demand, and jobs are aplenty. But when supply isn’t meeting demand, it becomes more difficult to do everything that needs to be done on the job. That gap is expected to widen to 1.5 million in the next five years, according to the most recent (ISC)² Global Information Security Workforce Study (GISWS) (https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)²-Global-Information-Security-Workforce-Study-2015.pdf).

(ISC)² is a leader in developing our next generation of cybersecurity professionals. As a community, we need everyone to join the battle not only to raise more cyber warriors, but also to sharpen our own cybersecurity swords by elevating our skills to the highest level.

INTERNATIONAL DEMAND FOR CYBERSECURITY

Study after study shows we’re lacking combatants on the cyber battlefield to take up both offensive and defensive roles. The 2015 GISWS, conducted by Frost & Sullivan, states, “Forty-five percent of hiring managers report that they struggle to support additional hiring needs, and 62 percent of respondents report that their organizations have too few information security professionals.” That this trend will continue into 2016 is supported by numerous other studies.

Questions remain:

• Where do we find this additional workforce?
• How do we ensure that their knowledge, skills and abilities meet diverse industry needs?
• What resources are at hand to teach both cybersecurity basics and the in-depth topics needed by industry?

To meet the need, we must start with the fundamentals of online safety, reaching out to everyone who is connected (and these days, who isn’t?). Then, we need to go beyond the security basics into the advanced topics required by today’s cyber workforce. We need to be able to reach people wherever they are and help them understand the security repercussions of life in the digital era.

EXTENDING OUR REACH

(ISC)² provides numerous ways to engage future professionals, from the Foundation’s Safe and Secure Online program for schoolchildren to the Associate of (ISC)² designation for those who pass certification exams but lack the minimum practical experience. Chapters also are working actively with high school and college students to help them enter the field and build career networks.

Valiant as these efforts are, we’re still not reaching enough students.

According to the 2013 Raytheon Millennial Cybersecurity Survey (www.raytheon.com/capabilities/ rtnwcm/groups/gallery/documents/digitalasset/ rtn_158203.pdf), “Eighty-two percent [of students] say no high school teacher or guidance counselor ever mentioned to them the idea of a career in cybersecurity.”

The Association of Computer Machinery and the Computer Science Teaching Association reported similar trends as early as 2010 in Running on Empty: The Failure to Teach K-12 Computer Science in the Digital Age. More recently, a 2014 Google and Gallup, Inc. study titled “Searchi
for Computer Science: Access and Barriers in U.S. K-12 Education” (www.gallup.com/opinion/gallup/184751/students-lack-access-computer-science-learning.aspx) came to a similar conclusion that more is needed to equip today’s students for tomorrow’s cyber world.

In the 21st century, no other subject provides as many opportunities as information technology/computer science, no matter the student’s ultimate occupation. Unfortunately, we’re failing on an international scale to provide students with even exposure to, let alone adequate education in, these subjects.

Failure is not an option, because, ready or not, the future has arrived.

JOINING FORCES IS CRUCIAL

It’s time for industry professionals to connect with educators, students and parents in order to meet the workforce needs of today and tomorrow. It’s not enough to leave this issue to teachers to resolve during standard classroom time.

• As concerned professionals, we must collectively go into our school districts and ask difficult questions about how, when and where they are teaching computer science, information technology and cybersecurity in K-12 classrooms.

• We must demand that schools move beyond the current basic technology literacy curriculum to ensure courses based on fundamental computing principles become part of the core curriculum (http://www.corestandards.org/).

• We need to ensure every child has access to a computer, because the only way for them to learn these concepts is through applicable instruction and hands-on activities.

See additional steps for taking action at http://services.google.com/fh/files/misc/searching-for-computer-science_recommendations.pdf.

ATTRACTING THE BEST AND THE BRIGHTEST

There are many ongoing activities that promote the next generation of security leaders, but we need cybersecurity coaches and mentors to guide these newcomers.

Conferences are getting kids involved in safe arenas to learn cybersecurity and practice their skills. Examples include the RSA Conference Cyber Safety Village, R00tz Asylum held in conjunction with BlackHat/DefCon and the Hak4kidz conferences. These kid-centered events are designed to spark children’s curiosity as ethical hackers in a safe and rewarding environment. Using nontraditional methods to engage kids with as much hands-on learning as possible, these events focus on areas kids care about and present them at a level they understand. They’ve reached thousands of kids, but they’re only scratching the surface.

Cyber competitions, clubs and camps go beyond the traditional classroom to grow students’ cybersecurity skills while developing professional traits. They promote both offensive and defensive skills to all ages and skill levels. [Examples include CyberPatriot (U.S.A.), CyberCenturion (U.K.), the MITRE Cyber Academy (with (ISC)²), National Collegiate Cyber Defense Competition (CCDC), and the U.S. Cyber Challenge (USCC).]

Dr. Dan Manson, the Cybersecurity Competition Federation director, sees cybersecurity competitions as “a learning sport providing real-world challenges leading directly into employment.” CyberFed (cyberfed.org/) is “an association of academic, industry and government organizations with a common interest in supporting cybersecurity competitions and the competitors they serve.”

CyberCompEx (https://www.cybercompex.org/) also focuses on developing the next generation of cybersecurity professionals tasked with protecting critical infrastructure and key resources. Karen Evans, director of both CyberCompEx and USCC, sees these efforts as a form of gamification of critical thinking skills through networking and collaboration.

WE NEED YOU

By joining these competition efforts, whether as a coach, mentor, sponsor or participant, you have the opportunity to sharpen your sword while making a difference. As (ISC)² members, your help is essential not only in reaching the cyber-ignorant but also in fostering those interested in cybersecurity as a profession. Consider partnering with teachers, school districts and community groups who are trying to make a difference. Help educate the educators, and let them know there’s a community who cares.

RON WOERNER, CISSP, CISM, CEH, is director of cybersecurity studies at Bellevue University’s College of Science & Technology.
MOST OF us have never played professional sports, but we can still identify with the kicker who misses a short field goal in the final seconds of the football game. Or with the golf pro who fails an easy-looking putt at the 18th hole. Similar anxieties can plague many of us, particularly when we’re placed in stressful situations. The key is finding ways to control, if not conquer, that angst.

UNDERSTANDING ‘TEST ANXIETY’

By definition, test anxiety is self-evident. You are nervous you won’t do well on an upcoming exam, especially one that has serious consequences. But the anxiety represents much more than that.

Yourdictionary.com defines test anxiety as “a fear of failing that you feel before or while taking an important examination that prevents you from performing as well as you otherwise could on the exam.” Of the many definitions you can find online, this one seems to capture it best.

One thing test anxiety is not is a judgment of your capabilities, according to Rachel Anderson, Ph.D., licensed counselor and instructor at the University of South Dakota. “It’s got nothing to do with ability. People experience test anxiety when they know they’re going to do great as often as when they know they’re going to do poorly.”
Test anxiety essentially is your brain on overload. Sian Beilock, Ph.D., director of the Human Performance Lab at the University of Chicago, has studied why people, from athletes to musicians to students, fail under pressure. She describes how stress impacts the brain’s “working memory” in the 2010 book *Choke—What the Secrets of the Brain Reveal about Getting It Right When You Have To*. “Working memory (cognitive horsepower) reflects our ability to hold information in memory...while doing something else at the same time.”

When we fall under extreme stress, Beilock says that part of the brain reacts negatively. “Being under pressure alters how different areas of the brain communicate” and the area that houses the working memory “stops talking to other brain areas that are also important for maximum cognitive horsepower.”

In other words, under stress, clear thinking is in danger.

**IT CAN HAPPEN AT ANY AGE**

Test anxiety is not uncommon. According to the American Test Anxieties Association, as many as 20 percent of K-12 students today suffer from a significant level of test anxiety.

Anderson says it’s also prevalent in higher education. “It’s become one of the more common problems on college campuses. With college students, anxiety has surpassed depression as the number one reason they come to [the college counseling center].”

Even those out of college—especially if it’s been awhile—can panic on the eve of an exam or performance test. “You may think, ‘Oh, I’ve had a few years under my belt. Test-taking is a skill-set that we learn, that we practice. If you haven’t taken a test in a few years, it’s going to feel very strange.'”

—RACHEL ANDERSON, PH.D., licensed counselor and instructor, University of South Dakota

**HOW 6 TIPS FOR DEALING WITH TEST ANXIETY**

_from the Anxiety and Depression Association of America_

1. **BE PREPARED**
   Develop good study habits. Study at least a week or two before the exam, in smaller increments of time and over a few days (instead of pulling an “all-nighter”). Try to simulate exam conditions by working through a practice test, following the same time constraints.

2. **DEVELOP GOOD TEST-TAKING SKILLS**
   Read the directions carefully, answer questions you know first and then return to the more difficult ones. Outline essays before you begin to write.

3. **MAINTAIN A POSITIVE ATTITUDE**
   Remember that your self-worth should not be dependent on or defined by a test grade. Creating a system of rewards and reasonable expectations for studying can help to produce effective studying habits. There is no benefit to negative thinking.

4. **STAY FOCUSED**
   Concentrate on the test, not other students, during your exams.

5. **PRACTICE RELAXATION TECHNIQUES**
   If you feel stressed during the exam, take deep, slow breaths and consciously relax your muscles, one at a time. This can invigorate your body and will allow you to better focus on the exam.

6. **STAY HEALTHY**
   Get enough sleep, eat healthfully, exercise and allow for personal time. If you are exhausted—physically or emotionally—it will be more difficult for you to handle stress and anxiety.
“You’re going into the testing center...you’re put in a room with other people who are taking the test. The pressure’s on. They’re not thinking the way they would when they’re at home in a comfortable environment.”

—DAVID L. PROWSE, former network administrator and consultant

I know what I’m doing’ that would decrease your anxiety,” Anderson said. “Test-taking is a skill-set that we learn, that we practice. If you haven’t taken a test in a few years, it’s going to feel very strange.”

**YOU’RE PREPARED—SO WHY ARE YOU SO ANXIOUS?**

Fear of failure is the key component of test anxiety. For people who have been relatively successful to this point, it’s also a fear of the unknown, Anderson observes. “What I find in common is that sense of ‘I’m going to fail’ or that fear of failure, that lack of experience in failure that can happen—we tend to be afraid of something if we don’t know what it’s going to look like.”

These anxieties can cripple confidence. David L. Prowse, a former network administrator and consultant, writes study guides for a variety of certification exams [but not for (ISC)² certifications]. He says environment can play a role. “They might be comfortable at home, and they might do well with the practice exams.”

But, when it comes to the real test in a different environment, everything can change, he warns. “You’re going into the testing center...you’re put in a room with other people who are taking the test. The pressure’s on. They’re not thinking the way they would when they’re at home in a comfortable environment.”

Psychologist Beilock agrees and writes, “When people practice in a casual environment with nothing on the line and are then put under stress to perform well...they often choke under the pressure.”

**GETTING THE BETTER OF YOUR TEST ANXIETY**

The big question at this point is: How do I control my test anxiety?

The Anxiety and Depression Association of America offers some tips:

- Be prepared by developing good study habits
- Stay positive
- Concentrate—don’t get distracted
- Get enough sleep; eat healthfully
- Relax through deep breathing, relaxing your muscles

In addition to the basics, don’t forget to take advantage of your experience.

“Look at where you’ve been able to be successful,” South Dakota’s Anderson said. “You don’t go in for certification exams unless you’ve had some success to build up that understanding. And allow that success to apply to the test.”

Taking a few minutes before your exam to write down your worries is another technique to control anxieties, suggests University of Chicago’s Beilock.

In a study at the university’s Human Resource Lab, students who wrote down their worries before a difficult math test scored about 15 percent better than the students who did not. “Disclosing negative information and labeling it as such frees your mind from unwanted thoughts and helps you focus on something other than the negative,” she concluded.

**BEATING THE ‘CHOKE’**

Anderson encourages test-takers to “normalize” the situation. “It’s OK to be anxious about a test.”

Admitting that test-taking is tough is not a weakness, especially if it gets you where you want to go. Using your skills, seeking guidance and having confidence seem to be the secrets to beating the “choke.”

---

DEBORAH JOHNSON is managing editor of InfoSecurity Professional magazine.
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
Time to Step Up Our Game

BY PAT CRAVEN

I KNOW YOU see it every day—the battle we’re fighting to keep the cyber world safe and secure is getting harder and harder. As a cybersecurity professional, you are doing your part to stop those who wish to cause harm to others. But, this isn’t a war you can win on your own. We have to do more to teach people how they can protect themselves and their families better. Here at the (ISC)² Foundation, we know we can do more to help, and that is exactly what we are going to do.

To position ourselves to have a greater impact within the community, the (ISC)² Foundation is changing its name to the Center for Cyber Safety and Education. We are revamping our branding and programs to expand our reach to the general public and provide them with the tools they need to stay safe and secure online. We know, however, that a name change or new website (www.SafeAndSecureOnline.org, which will launch in late March) alone isn’t going to solve all the problems. We need to back up our efforts with new and innovative ways to reach our communities.

The Center for Cyber Safety and Education just completed a study that will be released in the next few weeks about how children use the Internet. What makes this study unique is that we also interviewed the parents of the children and found there was often a big gap between what the children are doing and what the parents think the children are doing. Parents aren’t even aware that these gaps could be dangerous to their own children’s safety.

Armed with this data, we went to the 110,000 members of (ISC)² and picked the brains of the best cybersecurity professionals in the world. We have taken their tips and recommendations and are relaunching our Safe and Secure Online educational programs and making them available to everyone. Parents, teachers, group leaders—any and all of them—will be able to go to www.SafeAndSecureOnline.org and view or download programs and tips on how to protect themselves from cyber threats. The parents program will be the first to launch in the series.

Later this year, you will begin to see new videos, cartoons, games and even comic books featuring our new cyber safety “spokescat,” Garfield.

The Center for Cyber Safety and Education has entered into a partnership with PAWS, Inc. to produce a series of safety lessons for children featuring Garfield that will be in a variety of media and in various languages.

All of this is just the beginning. We are expanding our scholarship program to secondary and high school students through a new initiative called the Chapter Scholarship Challenge. And, we are hard at work on the next Global Information Security Workforce Study that we’ll release in 2017.

I encourage you to follow us on Facebook (search Safe and Secure Online) and Twitter (@ISC2Cares) and let us know what you think of the programs, show your support, and share with us any tips or suggestions you may have on how we can make a safer cyber world for everyone—together.
How did you first become interested in information security as a career?

I became involved in information security when I started my first job as a commissioned officer in the Royal Signal Corps of the Malaysian Armed Forces in 1987, after completing a bachelor’s degree in engineering from the University of Hartford in Connecticut (U.S.A.). I was fortunate to be selected as the Malaysian Armed Forces scholar. I have to admit that the American education system has shaped strongly my thinking process until today. While in the service, I completed my postgraduate diploma in system analysis at the University of Technology Malaysia, with an M.S. with distinction in information security from Royal Holloway, University of London and an MBA from University Putra Malaysia. I am still working on my Ph.D. with the National Defence University in Malaysia.

What would you consider your career high point(s) to date?

Briefly, my career has been divided into four areas: military service; government service; business development; and research and academic. Each one has had both high points and challenges. The first period was military service. During this time, I subscribed to the hypothesis that technology is an enabler and game changer to the organization. With this belief, I had been tasked to bring an information and communication technology culture into the military force, and it was a big challenge then, when most of the senior officers were seasoned counterinsurgency combatants.

I had to overcome their hesitations and prove that changes can be positive if taken appropriately. The successes came with the formation of appropriate establishments within the military force, and I received a service excellence award and fast promotions as a result. That was roughly a 12-year effort, and from this experience, I learned that every change has its timing, and we must keep on challenging it in order to succeed.

My second career area was with government-related companies, i.e., a research institution that led to the formation of a national cybersecurity institution. The culture within this realm was different than I experienced in the military arena. Thus, I realized we needed a new form of a cybersecurity agency at the national level—this time not fashioned from regulatory and bureaucratic perspectives, but rather from science and technology perspectives. As such, I focused on research, experimentation and innovation to address the dynamic threats of the cyber world. This was very exciting, since traditional security environments subscribed to an autocratic culture where command and control is fully exercised. We can never address the problems in the cyber world effectively, however, using this model.

Science and technology, R&D and innovation flourish better in a non-autocratic culture. This hypothesis led to the formation of a cybersecurity agency with science, technology and innovation at the forefront. I was privileged to lead this agency for 12 years, from cradle to adulthood. As a result of my efforts, I received the (ISC)² Harold F. Tipton Lifetime Achievement Award and many other honors. The sweetest memory is being able to visit the White House under the invitation of [board member] Howard Schmidt when he was the cybersecurity adviser to President Barack Obama.

My third career area was working with business enterprises. The challenges were different. I found that no
matter how wonderful our ideas were, and how good or secure our solution was, they had to fall back on business fundamentals, namely supply and demand, customers’ perceptions, resource limitations and time constraints. I was able to serve at least five cybersecurity companies—two of them outside Malaysia. By this time, I realized that business success is not entirely due to your own effort; many external factors come into play, such as being at the right place at the right time and knowing the right people. Despite many challenges, I received a prestigious Platinum Award by the Industry Association in Malaysia.

The fourth area is my current career in research and academics. I now have the chance to document key experiences into papers, journals and conference publications. A good part of this experience is to be able to conceptualize real-life experiences and to share them with students. I am a proponent of people-process-technology interactions, and my research focuses on information security in this context. This type of research is needed here in Africa.

What prompted you move to Namibia?
Mainly, the opportunity to apply my career experiences in the academic world and to live in a part of the world where information security education is strongly needed intrigued me. In this regard, I must thank Professor Jill Slay [a former (ISC)² Asia-Pacific Advisory Council member] and the Namibia University of Science and Technology for giving me the chance to be part of this dynamic academic team. I am very grateful and honored to serve this institution and interact with so many friendly people from Africa.

You can reach Husin Jazri at hjazri@nust.na or husinjz@gmail.com.
An expanded version of this interview will appear in the April issue of Insights, a companion eNewsletter for the (ISC)² membership.
Study for the CCSP exam with OnDemand training. This self-paced learning solution taught by Adam Gordon, (ISC)²-authorized instructor and key contributor to the curriculum, covers the 6 domains of the CCSP Common Body of Knowledge (CBK) in its entirety. Delivered in a modular format, this training allows students to spend extra time on material where needed and reinforce concepts with flash cards, quizzes, and games.

With the purchase of CCSP Training OnDemand, each student will receive:

- Official (ISC)² CCSP student workbook (electronic version)
- Interactive flash cards
- Post-assessment practice questions to gauge exam readiness
- 120 days of access to the recordings and course content from time of purchase

(ISC)² Members: US$395  |  Non-Members: US$495

Register Today
www.isc2.org/ondemand-training
Accepting candy from a stranger is no longer like accepting candy from a stranger.

Learn what the world’s leading cybersecurity professionals do to protect their kids from the dangers of the Internet. SAFEANDSECUREONLINE.ORG

CONTACT US AT: safeandsecure@isc2.org