BECOME A CYBER SECURITY LEADER

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

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

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
FEATURES

16 Saving Industrial Control Systems
What’s it going to take to put more power behind securing our critical infrastructure?  BY SHAWNA MCALEARNEY

20 The Rise of Multinational Malware
Two experts explain how to leverage language in digital forensics.  BY ONDREJ KREHĽ AND PAUL KUBLER

24 The NICE Way to Address Cybersecurity Shortfalls
Education is one way to ensure there are enough qualified professionals to fill the information security pipeline in the coming decade.  BY DOUGLAS MICHAEL RAUSCH

Cover photograph by JOHN KUCZALA  Illustration (above) by ENRICO VARRASSO
Editor’s Note

TIME TO POWER UP
Educating legislators will help them craft better laws

AROUND 3:30 P.M. on Sept. 8, 2011, I was sitting in a sunlit San Diego conference room when the power went out. The meeting continued despite the setback until someone came in and suggested we leave. The power was out everywhere, and people were starting to panic.

Getting home took hours, mainly because there were no traffic lights to manage manic drivers and growing gridlock. The freeways were less of a free-for-all, but dozens of drivers abandoned their cars after running out of gas. Every single business closed. No gas stations or public transit. No grocery or convenience stores. No restaurants or pharmacies. One major hospital even had trouble with its backup generators.

Given that it was just days before the 10th anniversary of the 9/11 U.S. terrorist attacks, everyone initially thought the Southwest Blackout, which remains the largest power failure in California history, was intentional. News agencies later reported a lone Arizona utilities worker made a cascading error while working on a power line.

Since then, I stopped taking the grid for granted. This issue’s cover story is yet another reminder of how important it is to continually protect our critical infrastructure from cyber attacks. Whether you work in the public or private sector, sealing up those systems’ vulnerabilities is important to us all.

So is openly discussing what is—and, frankly, what isn’t—working in the security world. Later this month, (ISC)² members will have an opportunity to initiate or join some of those discussions as they gather in Washington, D.C., for the CyberSecureGov conference. These are important talks, given that some of the biggest data breaches last year involved U.S. government agencies. Some of our biggest privacy concerns involve government, too.

Let’s collectively better educate our legislators on what is really happening in cybersecurity so they can craft legal solutions that truly protect citizens and minimize potential consequences. Both elected and appointed officials tend to listen to whomever speaks loudest. So, speak up when the opportunity arises. It’s time those in the trenches had a stronger voice.

> 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
(ISC)² ........................................... 7
(ISC)² ........................................... 12
Onapsis ................................................................. 14
(ISC)² ....................................................... 15
(ISC)² ....................................................... 23
(ISC)² ....................................................... 27
(ISC)² ....................................................... 29
Twirling Tiger Media ........................................... 31
(ISC)² ....................................................... 32

© Rob Andrew Photography

InfoSecurity Professional  •  4  •  May/June 2016
THERE’S NO SHORTAGE OF CYBER SECURITY THREATS

BUT THERE IS A SHORTAGE OF IT SECURITY PROFESSIONALS

DO YOU HAVE WHAT IT TAKES TO BE PART OF THE SOLUTION?

Get up-to-date security skills with Capella University’s Master’s in Information Assurance and Security (MS-IAS).

Specializations include Digital Forensics, Network Defense, and Health Care Security.

Along the way to your MS-IAS, earn up to 3 NSA focus area digital badges showcasing your mastery of skills in specific cybersecurity areas.

Plus, the knowledge you gained for your CISSP®, CEH®, or CNDA® certifications can help you earn credit toward your MS-IAS, saving you time and money.

ANSWER THE CALL. START TODAY. CAPELLA.EDU/ISC2 OR 1.866.933.5836
(ISC)² MEMBERS REPRESENTING all facets of government and beyond will gather May 19 and 20 for the fourth annual (ISC)² CyberSecureGov conference (http://cybersecuregov.isc2.org) at the Washington Convention Center in Washington, D.C. Keynotes, panels and presentations will focus on game-changing solutions that can shake up the status quo. This is an important opportunity for our members to learn from each other and other experts how they can set a new course toward a stronger government cybersecurity posture.

Everyone’s tired of breaches. The protections we erected in the past aren’t working so well now and no doubt will fail to protect our networks and critical infrastructure going forward. Taking two days to meet with fellow practitioners and experts in both the public and private sectors, military and academia can help not only those working in a government support capacity but also the tens of millions of citizens who use government services.

The conference will bring together experts from all over—not just government circles—to share best practices and to brainstorm ways to get ahead of ever-evolving cyber attacks that continue to plague our systems.

Among those with a presence will be members of the Institute for Critical Infrastructure Technology (ICIT) (http://icitech.org/), a Washington-based, nonpartisan think tank, of which (ISC)² is a fellow. By partnering with ICIT, our organization is able to connect with the legislative community and better educate lawmakers who propose cybersecurity-related bills on Capitol Hill. It’s important that elected officials and policymakers understand the impact these proposed bills have on our industry and the verticals that fall under them.

Laws are not the silver bullet, of course, but well-conceived, well-constructed laws and regulations can help improve security standards across the spectrum.

We also need enough qualified people working within organizations to provide a broad range of security services—from carrying out regulations to assessing risk and managing security operations. That’s why it’s important for us to continue to work to fill the 1.5 million open jobs expected by 2020—and with qualified, highly motivated professionals with the capacity and resources to build a career in information security.

By partnering with ICIT, our organization is able to connect with the legislative community and better educate lawmakers who propose cybersecurity-related bills on Capitol Hill.

I’m particularly glad that members of the International Consortium of Minority Cybersecurity Professionals (ICMCP) (https://icmcp.org/) also will be at CyberSecureGov. (ISC)² and ICMCP have complementary missions, and together, we can develop ways to draw more underrepresented minorities, women and people from economically challenged areas to work toward a fulfilling career in information security.

A more diverse workforce generates more ideas based on different perspectives, experiences and approaches to common problems. Working together, we can each do our own small part to make the cyber world a little safer. Whether you work for IBM or the IRS, now is the time for each of us to find more effective ways to stop cyber attacks that continue to leave tens of millions of citizens at risk. ©
Broadcast your accomplishments with digital badges.

(ISC)² has partnered with Acclaim, a product of Pearson, to deliver a standardized way of digitally representing your certifications and accomplishments in a verified manner.

Claim your (ISC)² digital badge and benefit:

» As a Job seeker – Tell the full story of your professional life with verifiable information

» Employers – Can easily evaluate and validate the qualifications of job applicants

» Get noticed by sharing badges on LinkedIn, Facebook, Twitter and more

You’ve invested time, energy and money into preparing yourself for a great career opportunity; make sure the right people in the right places value it. Digital badges put you in control of where and how you share your potential.

LEARN MORE:
www.isc2.org/digital-badges
(ISC)² NAMES NEW SENIOR MANAGER OF EDUCATION

MIRTHA COLLIN, formerly the executive director of enrollment and program management for innovative education at the University of South Florida, joins (ISC)² as senior manager of education. In this role, Collin will be responsible for the creation, support, maintenance and delivery of (ISC)²’s current and future credential programs, developing key strategic partnerships for rich content, and evolving (ISC)²’s learning environment and toolsets to be an industry leader. She will work closely with (ISC)² teams to ensure that quality, consistency, compliance and governance rise to a higher standard.

Collin brings vast experience in identifying new markets, working with faculty and instructional design staff to develop relevant and in-demand courses and programs, and recruiting students, among other skills. At USF, she served as special assistant to the provost and was primarily responsible for activities related to senior-level academic administration.

Prior to joining USF, Collin held a number of positions at Harvard University, including senior project manager for Harvard’s Office of the President and Provost and senior campus planner with Harvard’s Allston Development Group (ADG), a project to expand Harvard’s campus.

A graduate of Wellesley College, Collins earned a BA in psychology and a master’s degree in city and regional planning at the University of California, Berkeley.

ONE MEMBER’S STRESS-BUSTER: MEDITATION

Work, home—life in general—can create a perfect storm of stress-related conditions. In the search for ways to control the stress in our lives, we often reach out to see what our colleagues, friends and family members have discovered. Looking to share some of these solutions, InfoSecurity Professional is launching Stress-Busters.

In this entry, (ISC)² member J. Allen Valentine, CISSP, offers meditation as a way to manage stress. A 20-year security practitioner, Valentine says the benefits he has derived include increased focus and reduced anxiety.

His specific form of meditation is heartfulness—a meditation on the heart. He offers this description:

“We sit in a relaxed pose and imagine a light in the heart. As thoughts arise to distract us, we treat the thoughts as uninvited guests and return to our imagining light in the heart. I personally think of these thoughts as ‘barking dogs.’ They are distractions to which I should pay no attention.”

Meditation is one of many practices people have adopted to help cope with stressful lives. Valentine offers his experience as something that’s worked for him. For more information, you can visit www.heartfulness.org.

Do you have a stress-buster you’d like to share? Drop us an email at djohnson@twirlingtigerpress.com.

HE SAID...

Our problem is not a technology problem. Our adversaries are not beating us because they have better technology. They are beating us because they are more creative.”

—AMIT YORAN, president, RSA, speaking at RSA 2016, San Francisco, CA
RECOMMENDED READING

Security Risk Management  By Evan Wheeler
Suggested by Larry Marks, CISSP

As a risk management professional in information security, risk and governance, I needed a top-down reference to use as a ready guide to help refine and re-energize my company’s risk management program. I found it in Security Risk Management: Building an Information Security Risk Management Program from the Ground Up by Evan Wheeler, an expert in information security and operational risk management. Wheeler also wrote the Information Security Risk Management course at the SANS Institute.

This much-needed approach to information security presents ready-to-use templates and a road map to help implement a risk management program. The Appendix is this book’s sweet spot to jump-start a risk assessment of an application, system or piece of hardware:

- Appendix A consists of a Sample Security Risk Profile, with fewer than 20 questions to opine on the risks.
- Appendix B provides a risk scale that the reader can use to generate an extensive or shortened version of a heat map.
- Appendix C, Security Enhancement Levels and Sample Network Security Controls, provides instances of controls the reader can use to review or vet controls as part of the risk assessment of the enterprise.

A caveat about an otherwise excellent guide: As this book was published in 2011, there is little coverage of cloud risk assessment or vendor or third-party risk assessments. For a detailed how-to on setting up or revitalizing a risk management system, however, Security Risk Management is a definite asset to your technical library. ●
MEMBERS OF THE (ISC)² Hellenic Chapter haven’t let the well-publicized economic challenges in its country curb their ambitions. With its strong foundational membership and a successful sponsorship program for their education events, the chapter has now become the third official (ISC)² training provider in the EMEA region.

The chapter’s board and membership decided that career support for Greek professionals should be a core objective. The development of an accessible, cost-effective route to certification for the Greek market provides an important advantage for those professionals looking to move into lucrative roles outside of the country, says chapter president Konstantino “Kostas” Papadatos, CISSP.

“There is so much demand both inside and outside of Greece for experienced people, and formal certification is a great asset to professionals looking to explore these opportunities.”

—KONSTANTINO PAPADATOS, chapter president

“There is so much demand both inside and outside of Greece for experienced people, and formal certification is a great asset to professionals looking to explore these opportunities,” Papadatos says. When asked if an exodus of professionals is a concern for the chapter or Greece, he confidently responds, “Not at all. Many will come back stronger and will be an asset to the country. We are happy to be able to help professionals pursue their ambitions and build their careers.”

The chapter has made progress despite the turmoil in Greece. Though it received its charter nearly two years ago, it took almost a year for various government bodies to formally recognize the chapter.

Papadatos recounts the challenges. “When we finally got the initial approval, we had to conduct our general assembly and elections amidst a national referendum—and at a time when we were unable to open a bank account and people faced cash withdrawal limitations due to banking capital controls,” he explains. “We were not sure if our members would be able to withdraw the cash to pay their annual fees during registration. In spite of our fears, we not only successfully conducted our general assembly but also gained our first 50 members and five sponsors supporting our event.”

The chapter also is actively liaising with universities that have information and cybersecurity courses to encourage certification for students. It is keen to support development of the International Academic Program (https://www.isc2.org/international-academic-program/default.aspx) within Greece. As a result, there are about 15 students within the membership, many of whom are interested in certification.

The chapter aims to offer evening educational meetings and panel discussions every two or three months. “We are an experienced community, very motivated to do the best for Greek professionals. I think we can be proud of the achievement so far, and that makes us confident for the future,” its president says.
(ISC)² TEAMS UP WITH ASIS INTERNATIONAL AND ISACA

ASIS International (ASIS) (www.asisonline.org), (ISC)² (www.isc2.org) and ISACA (www.isaca.org), the professional associations for physical, cyber and information security, will collaborate on a Security Awareness American National Standard. This guidance standard aims to address the intersections of physical, cyber and information security management and to help organizations of all sizes maximize protection of human, tangible and intangible assets.

In an increasingly complex and interconnected world, the public and private sectors face growing physical and electronic challenges to protect personal information, business transactions and critical infrastructure. It is essential that organizations of all types and sizes have the best tools at their disposal to promote security awareness from a holistic perspective.

"Businesses are struggling to cope with all of today’s security threats," says Dr. Casey Marks, the director of (ISC)² Examinations Department. "The continued convergence of cyber and physical security causes our adversaries to neither think nor act in silos when they perform malicious activities. An all-encompassing security standard like this will help to provide businesses with needed guidance. We’re pleased to be a part of this effort with two well-respected industry organizations."

The standard will focus on cross-disciplinary management measures, as well as awareness and training programs to help organizations and their supply chains prepare for and minimize the likelihood of an undesirable event, as well as respond to and recover from a security incident.

ASIS, (ISC)² and ISACA will form a joint technical committee and working group to develop the standard and solicit input from security experts around the globe. The committees will operate under ASIS’s ANSI-certified process (https://www.asisonline.org/Standards-Guidelines/Resources/Documents/ASISSTDPROC5%20v1%20without%20track%20changes.pdf) to develop an ANSI American National Standard that can be applied worldwide.
Build Better Software
Train Your Team to Develop Secure Code

The Secure Software Practitioner Suites are a series of OnDemand learning courses that teach foundational elements of software security and language-specific secure coding. Each suite of courses is catered for specific roles, breaking down the learning so users efficiently learn only what they need. Following the course, users validate their skills by passing an (ISC)² certificate exam.

Specialized suites offered in:

- **JAVA DEVELOPMENT**
- **MOBILE DEVELOPMENT**
- **PHP DEVELOPMENT**
- **.NET DEVELOPMENT**

Learn More
www.isc2.org/secure-software-practitioner
Privacy: Foundation or Faux Pas?

It’s time to closely evaluate existing privacy laws in the United States.  

BY GORDON MERRILL

WHEN I WAS a little boy, I remember being taught about a song that said, “the wise man built his house upon the rock” and “the foolish man built his house upon the sand.” The rains came, and then floods came, and “the house on the rock stood firm,” while “the house on the sand fell flat.” When it comes to privacy, which foundation are you working with?

To help answer this question, here’s a quick recap of some basic points on the foundation of privacy that we IT security professionals know but may need be reminded of from time to time:

• There are two foundational concepts related to the privacy of personal information: opt in and opt out.
  – With opt in, you have the ability to grant a person or a group the right to use the parts of your data that you specify for an intended purpose and only for the amount of time that you specify.
  – With opt out, anybody who possesses information about you is able to hold onto it and do with it what they want without your knowledge, permission or approval.
• In order to actually opt out, you have to know who possesses data about you and petition him/her to remove it, quit using it and destroy it in order for you to regain control of your privacy. Are we starting to see a rock and sand foundation analogy here?

I’ve had occasion to see opt-in enforcement firsthand. My wife and I vacationed abroad and bought matching souvenirs. We hadn’t been back home a month before one piece from the set was ruined. I notified the shop where we purchased the set, and they sold and shipped a replacement item. About a week after the sale, the shop contacted me by email every day to try to confirm receipt of the item. As soon as the transaction was satisfactorily completed, the company was mandated to remove my data from its records. They were authorized to have it on file since I requested a sale and shipment, but as soon as my transaction was complete and the receipt of my shipment was confirmed, the authorization to hold my data ended, and all data was removed from their records.

How completely different things are in the United States, where we are clearly defined at the federal government level as working from an opt-out “foundation.” With opt-out, you probably do not know who currently possesses data about you. If you don’t, then by default, opt out allows third-party companies the right to use your private data as they wish until you specifically request that they stop. We can only gain control of our own personal data if we know who all possesses data about us.

However, since there is no legal reason to force people or businesses
to remove your data after they’ve used it, can you even guess where all of your data is stored? Elementary schools, applications for groups, sororities, previous girlfriends/boyfriends, car dealers, pharmacies, etc. So if you don’t know where all of your data is, and you can’t therefore petition companies and/or people to force them to remove it, they can continue to retain it by default.

The U.S. Supreme Court ruled decades ago that third-party data holders have no obligation to protect your data by maintaining privacy, to ensure the data is accurate, or to accept any liability if that data is false and causes harm.

In a piece I wrote for the February 2016 Insights e-newsletter (https://www.isc2.org/infosecurity-professional-insights.aspx), I discussed some of the root causes of digital crime issues in our connected society. The fact that we do not have laws in the U.S. that allow us to treat digital data and crimes like we do analog crimes has severely weakened our ability to pursue the true criminals and has instead led us down a path to criminalize victims of digital crime. Add to that the lack of regulation on personal privacy and the federally sanctioned business of buying and selling data with no responsibility or liability, and we see how we are actually producing a climate that makes it difficult to pursue and prosecute the real criminals brokering our personal data. The big concern is that we hear about the crimes against businesses like Home Depot and Target, but we never hear about the digital crimes against citizens that cause people great personal, professional, financial and even career harm.

Merriam-Webster calls a faux pas an “embarrassing social mistake.” It appears that our head-in-the-sand approach to protecting citizens and their data has led to a major,
embarrassing social mistake. Our foundation of opt out has actually set the stage for our faux pas of privacy, which has forced us to opt out of personal privacy.

Decisions are made about us by businesses routinely from searches of databases internationally, for which we do not have full disclosure of who possesses our data, why they have it, whether it is correct or not, and little to no recourse if it is incorrect. So, if I don’t get a job I am fully qualified for based on data sold by a service that happens to be false (and can be proven so), why is no one held responsible, and further legally liable, for that error? What about the financial exposure derived from that false data that a broker freely trafficked to make money? If I made seriously false statements about a person in the local paper, I would be liable for defamation. But, if I sell false data, I am protected as a third-party data holder. So we’re left with a fundamental question: Why do we continue to allow our digital data to be treated differently?

True security professionals like us, as I wrote previously, “face true threats not only from cyber crime, but also from civil penalties when we are victimized by criminals we can’t pursue, and are outnumbered to defend against.” Only now, it’s personal—we are not allowed to protect our own data or keep our private data wholly private.

So, what kind of foundation does this put personal privacy on? Picture yourself advancing to the next level of your favorite strategy video game, and on this level, we add the difficulty of making you build all of your security on a foundation of sand, which we know will fail when the storms of cyber crime attack. So why did we get into this line of work again? Well, that is a subject for another day.

NEW On-Demand Training

Anywhere, Anytime, AT YOUR OWN PACE.

(ISC)²’s new OnDemand Training is a self-paced learning solution delivering modular training combined with interactive study materials, giving you a powerful alternative to traditional classroom training. Spend extra time on material and reinforce concepts with flash cards, quizzes, and games.

Learn more at » www.isc2.org/ondemand-training
“Power Grid in Ukraine Hacked.”

“Ukraine Fights Off Attack on Donetsk Airport.”

These are just the latest noteworthy attacks involving industrial control systems (ICS), and while they were both in Ukraine, it’s only a matter of time before it happens in the United States and elsewhere—and possibly on a much larger scale. Despite years of attempts (and likely some secret successes) by malicious hackers using tools like Stuxnet, Flame, Havex and Black Energy, many systems remain vulnerable. What could such an attack accomplish that would impact our lives and our businesses, and what can security professionals do about it?
First, let’s look at ICS, which encompasses everything from building facilities to airports to space stations. And a particularly rich source of vulnerabilities is the ICS subset SCADA, or Supervisory Control and Data Acquisition, which is used for geographically widespread ICS systems like pipelines and power transmission. Both ICS and SCADA systems are vulnerable to insider threats and multiple attack vectors, but ICS experts say some systems also use computers running proprietary software that are vulnerable to both targeted malware and more general malicious code in the wild.

“From the electric grid to oil and natural gas pipelines to embedded systems within industrial controls, there are many different vulnerabilities to address,” says Dan Lohrmann, chief security officer of Security Mentor, Inc., who also led the state of Michigan’s cybersecurity and technology infrastructure teams for a dozen years. “A few prime targets include power grids, military equipment, refineries and air traffic control systems. When enough vulnerabilities are found by some adversary to cause a major outage, we could have a major event rivaling September 11th.”

If successfully attacked, the repercussions could be quite substantial. “If [power plant] systems using SCADA are hacked,” warns Alan Paller, president of the SANS Technology Institute and director of research for the SANS Institute, it would “damage generators in dozens of power-generation plants. Because we have no more than one backup generator in reserve, power could be out for months—many months.”

If successfully attacked, the repercussions could be quite substantial. “If [power plant] systems using SCADA are hacked,” warns Alan Paller, president of the SANS Technology Institute and director of research for the SANS Institute, it would “damage generators in dozens of power-generation plants. Because we have no more than one backup generator in reserve, power could be out for months—many months.”

“Targets of those who are economically motivated could be oil and gas companies, large manufacturers and data centers of large financial institutions for sabotage, espionage or theft of sensitive information,” explains Galina Antova, a leading ICS expert and co-founder of Team8 Industrial. “Politically motivated actors—such as nation states—are likely to target the electrical grid, transportation hubs and anything that is critical to the infrastructure of a country.”

The viability of those targets has gained more credence with recent attacks on both the power grid and an airport in Ukraine.

Lohrmann concurs, stating, “There is a fear that ISIS [Islamic State of Iraq and Syria] or other terrorist groups are trying to gain the ability to attack SCADA systems. But while this is in the early phases, it could become a major threat in the future as more and more countries try to grow their capabilities in this area.”

Attackers are looking at a big payoff that doesn’t rely on a great deal of skill, making their goals—whatever they are—easier to achieve.

“The sad thing about our industry is that to hack into an ICS network is, in most cases, less challenging than to get into an IT network.”

—GALINA ANTOVA, co-founder of Team8 Industrial

**INDUSTRIAL ATTACKS ON THE RISE**

A 2015 Trend Micro survey of more than 500 security chiefs across 26 countries in the Organization of American States (OAS) reports that more than half saw an increase in cyber attacks against critical infrastructure during the past year, including attackers trying to “manipulate equipment” through an ICS. Forty percent said attackers had attempted to shut down computer networks altogether, and 44 percent of survey respondents said attackers tried to destroy information.

Lohrmann says that awareness of ICS security issues has improved since Stuxnet and other similar attacks failed to take down the power grid and nuclear facilities. “But the bad guys are getting better as well,” he said. “There are also more potential bad actors involved.”

For example, ICS experts say that Black Energy is a real threat to SCADA systems and is quite widespread.

“Black Energy is currently resident on a tremendous...
number of networks that control or monitor critical infrastructure such as electricity,” Dr. Phyllis Schneck, deputy undersecretary for Cybersecurity and Communications for the National Protection and Programs Directorate (NPPD), said in a recorded discussion with Lohrmann.

In that talk, Schneck, who also is the chief cybersecurity official for the U.S. Department of Homeland Security, said the notion of dormant malware meant to create an uncontrollable event in critical systems is not only simply frightening but also demonstrates two key points:

• Many are unaware of the control others may have over the systems that affect our way of life.
• Such widespread adversarial access to our systems is why we need resilience. “We need to accept that many electronic systems are open and vulnerable, and we need to take risk mitigating steps to protect them, while being ready to operate under attack.”

“There are two types of ICS owners and operators—those that are breached and know it, and those that are breached and don’t know it,” says Antova. “Whether it’s just a script kiddie playing around or APT resulting in infiltration of info or sabotage, most major organizations have some kind of breach that has occurred in their facilities.”

That lack of awareness fuels the scope of the problem. By not knowing their systems have been breached, ICS operators allow an attacker to sit and eavesdrop or run a payload whenever the time is right.

“Breaching security inside power companies and installing malicious software that hides effectively from common defensive tools and is ready for the attacker to mobilize when he or she chooses provides a mechanism for taking out power either for leverage in international conflicts or to prepare for war,” Paller says.

CHALLENGES IN SECURING ICS

With so many known breaches and vulnerable targets for which an attack could be disastrous, why does securing ICS continue to be such an issue? Experts say the design cycle/life cycle is a problem, proper security measures aren’t in place, and there are always worries about system availability.

“Industrial Control Systems were not meant to be networked, so when they started getting connected to networks, that posed new challenges in securing them,” Antova says. “The life span of those systems is usually 20 to 25 years. Since ICS networks are usually poorly segmented, if at all, attackers find it much easier to move around these networks, which are not monitored. That makes attackers harder to spot. Industrial protocols are not encrypted, and most controllers don’t use strong authentication, so hacking programmable logic controllers is not really hacking; it’s more akin to just telling the controllers what to do.

“These factors make ICS networks relatively easy to penetrate,” explains Antova. “Once the attacker gains control,
there are a number of ways in which he can cause physical damage by changing the process itself and instructing the PLCs to perform actions that result in physical damage.”

Antova believes the ICS vendors are trying hard to improve, but design cycles pose challenges (it usually takes five years to design a new controller), as well as the 20- to 25-year life cycles of ICS systems. Infosecurity professionals need to view the system and the network as a whole rather than look at endpoints.

“I spend a lot of time thinking about how we can do better at protecting our critical infrastructure and lower those risks,” she says. “Unfortunately, given the poor state of the industry, something bad is bound to happen. In many cases, the industry is still waiting for a major event to use as a justification to start spending and proactively addressing those challenges.”

**ALL ABOUT THE MONEY**

When examining the complexity of a SCADA system and the volume of potential weak points, cost is one of the first issues that leaps to mind.

“The scariest problem with SCADA right now is the enormity of the installed base with cyber vulnerabilities,” Lohrmann says. “There is a huge, aging infrastructure, and the cost involved with fixing these problems is immense. However, owners and operators of SCADA want to mitigate these threats gradually over time. It is like having cuts all over your body but only a handful of Band-Aids. Which cuts get the needed attention?”

Antova believes the solution is not necessarily throwing more money toward security measures but rather reassessing and reallocating current resources to “appropriate” technologies.

“Having better security does not necessarily mean spending more money,” she says. “First, there are a lot of policies and procedures you can implement that do not require capital expenditure investment. Second, chances are industrial customers are spending money on the wrong type of cybersecurity software for their ICS networks.”

And investing in the “wrong” security tools can impact more than the budget; it can also result in a more vulnerable network if the tools aren’t used.

“If they are just buying off-the-shelf IT-type tools such as IPS [intrusion prevention systems], their operations team will never allow those to be deployed in the lower levels of ICS networks because those types of solutions are not passive and don’t understand industrial protocols at those levels,” says Antova. “Organizations need to see where they are already spending money on ICS cybersecurity measures and maybe redirect them to the appropriate measures and technologies.”

And last but by no means least, security protection is crucial, but it is not the only issue. Paramount to both the owner/operator and their client base is the availability of those processes and ICS networks. Security measures that impede availability simply won’t be used.

**DEFENDING ICS**

So, what can we do to harden ICS from a growing number of sophisticated attacks? Start with the basics:

- Gain visibility into ICS systems and monitor them
- Implement proper asset management practices
- Separate networks

Also, use solutions that provide enhanced availability through early detection of cyber threats or by optimizing operational performance through measures such as compliance reporting, change management control and detection of user errors.

“ICS and SCADA security are lagging significantly behind the state of IT security,” Antova maintains. “To get us closer to the modern age, we need to start examining the guts of those ICS networks and be able to discern when there is abnormal activity. Machine-to-machine communication patterns are much more predictable than in the IT space, and we can achieve a lot more using behavior analytics and anomaly detection, implementing security measures in a way that does not disrupt operations of ICS networks.

“Let’s not forget that their primary purpose is to run critical processes.”


“As in the IT domain, so, too, in the ICS space, breaches are inevitable. An attacker with significant time and resources will always find a way in,” Antova says. “But what matters is how fast you can detect them when they get into your ICS networks.”

Our critical systems are vulnerable, and attackers are out there waiting for the right time. Will it take a cyber 9/11 to move ICS security forward?

“I think we need to take these threats seriously,” concludes Lohrmann. “Do I think it is likely to happen soon? Not necessarily, but we still need to prepare, just as we would for natural threats like hurricanes in Florida.”

SHAWNA MCALEARNEY is a freelance writer from Massachusetts.
THE RISE OF MULTINATIONAL MALWARE

BY ONDREJ KREHEL AND PAUL KUBLER

NATIVE-LANGUAGE TOOLS and exploits have recently started gaining momentum in the ever-growing sphere of multinational cyber crime, as hackers develop their own tools and in their own language. It’s common knowledge that much of the malware we discover today is written by non-English-speaking authors. In fact, Eugene Kaspersky, speaking to the Australian National Press Club two years ago (http://qz.com/146099/half-of-all-computer-malware-is-written-in-chinese-but-the-most-dangerous-is-written-in-russian/), pointed out that more than half of all malware is written in Chinese, followed by Spanish, Portuguese and Russian, respectively.

Figuring out who is behind an attack is important for responders classifying risk. Is this a group behind a major APT breach, or is it a copycat in some other country? Does it originate in a country that is well-funded in terms of attacks, or is this a group that’s emerging or unsupported?
Kaspersky was merely referring to the language used by the authors in their comments, but we have recently observed an increasing amount of malware containing large amounts of foreign languages (that is, languages not common to the nation where an (ISC)^2 member works). The forensics practitioner analyzing such malware code must be skilled in recognizing these languages and proficient in translating them precisely. One must be careful, however, not to assume that the easy discovery is the only discovery. For example, if someone discovers a Mongolian-language exploit comment, a digital forensic examiner can search for common words in that language, but this may cause the examiner to overlook a new language, such as Pashto, which the author used on top of Mongolian.

**TRYING TO EXTRACT THE MOTHER TONGUE**

The use of foreign languages may not necessarily mean that the authors are from a country that speaks those languages. Instead, it may be an intentional planting into the code syntax and words that point to a different country or an ethnic group, as was observed in the Mask APT (a.k.a. “Careto”). In Spanish, careto translates to “mask,” and it was one of the top APT campaigns discovered in 2014, the quality of which is said to be close to the capabilities of intelligence agencies. Experts believed that a Spanish speaker created the code due to the references in it ([arstechnica.com/security/2014/02/meet-mask-possibly-the-most-sophisticated-malware-campaign-ever-seen/](http://arstechnica.com/security/2014/02/meet-mask-possibly-the-most-sophisticated-malware-campaign-ever-seen/)).

The Mask is not the only such campaign—far from it. And, with each similar outbreak, it is difficult for digital forensic investigators to accurately determine the origins of the malware in question.

Determining the source of malware based on the code alone may prove to be difficult and inaccurate, as we can observe in the analysis of the cyber espionage group APT 28. An in-depth report on APT 28 by FireEye ([https://www2.fireeye.com/apt28.html](https://www2.fireeye.com/apt28.html)) revealed pinning the operation on Russia required a bit more effort than usual. To determine the location of the creators, it was necessary to match the compilation times of the malware over the years to a specific time zone based on typical work hours. Based on this information, it would appear that the attackers are located in Moscow and St. Petersburg. It’s this type of critical and investigative thinking that digital forensics examiners must use in their investigations.

**MORE THAN MERE MALWARE AT STAKE**

In addition to malware, cyber attackers are developing similar tools in local languages. An Iranian cybersecurity firm called ITSecTeam developed such a tool. Their tool, named “Havij” (which translates into “carrot”), is a SQL injection tool popular with cyber criminals across the globe. Upon our first encounter a few years ago with a command-based version of the tool, we examined the source code and saw what appeared to be Iranian strings, giving us clues about the origins of the authors.

The expansion of native-language malware and tools changes how both attackers and forensic examiners can leverage language to their advantage. If a known adversary is from Portugal, automatically filtering for Portuguese may help in discovering that enemy and potentially give an examiner insight into the nature of the group. A smart malicious hacker can, however, shy away from Portuguese and English tools in favor of those written in a more unexpected language, such as Swedish, to escape detection. Attackers can also write tools in their own languages, obviating the need to know English and opening the field to more people.

Typically, we can split cybercriminal groups into three categories based on funding and skills, which impact their effectiveness. Language clues left behind in the malware source code make it easier to determine whether the perceived attacker is indeed behind the attack.

**Retired state-sponsored:** This is typically the most dangerous and rightly feared category. These groups are
Various organizations are monitoring information trading over the TOR network to gather information on the latest data breaches.

well organized and have massive knowledge and resources to back them up, enabling them to carry out long-running covert missions. They are mostly focused on cyber espionage, stealing sensitive data for major financial gains and using creative tactics.

Organized cybercrime: Organized crime leaders recognize cyberspace as a new frontier for criminal activity and have moved swiftly into this relatively new territory in hopes of increased earnings. These groups typically focus their attacks on private organizations for financial gains. They can have major funding as well and may use creative ploys to access sensitive data illegally.

Small-time cyber criminals: These are not usually well organized and often not very creative, usually reusing the tools created by malicious hackers. They can, however, easily cause serious damage. Many low-end tools are the costliest to victim companies if criminals use them on a large scale.

COMMUNICATING THROUGH A STYLE ALL THEIR OWN

Similarly, we can observe multinational diversity in online forums targeting speakers of specific languages. By using slang and Internet/SMS-style language, the cybercrime community can communicate in ways that fly under the radar of an automatic translator but that native speakers still understand. Even the United States Central Intelligence Agency has a difficult time finding native speakers and currently runs a massive recruiting program (www.reuters.com/article/us-usa-cia-idUS-TRE5AQ2N220091127) to attract Arabic speakers to infiltrate such forums effectively, an investigator needs to pass for a native. The language-specific nature of these forums makes the job harder for examiners combing through forums to get tips on the latest exploits and movements or trying to understand a group or tool in action.

Various organizations are monitoring information trading over the TOR network to gather information on the latest data breaches. Without access, however, they might not notice much of the data. Local law enforcement agencies are now stepping in to help keep track of locally operated underground markets and forums.

While the shift to using local languages in tools and forums makes it harder for forensic investigators to track cyber criminals, it’s now easier for local law enforcement officials to tackle local cyber crime. Instead of having to learn English, these authorities are able to conduct investigations in their native languages. Local language, however, only partially masks activities and missions.

The English language and the universal language of computer code are still the prevalent forms of computerized crime code. In the future, one could predict that only the combination of English, computer code knowledge and the native language of an attacker can efficiently solve computer crime cases. Having a local native component of understanding might be at least as or even more significant than the rest.

ONDREJ KREHHEL, CISSP, CEH, CEI, EnCE, is the CEO and founder of LIFARS LLC, an international cybersecurity and digital forensics firm. He’s the former CISO of Identity Theft 911, an identity theft recovery and data breach management service. He previously conducted forensics investigations and managed the cybersecurity department at Struz Friedman and the Loews Corporation. With two decades of experience in computer security and digital forensics, he has launched investigations into a broad range of IT security matters, from malicious hacker attacks to data breaches to intellectual property theft. His work has received attention from CNN, Reuters, The Wall Street Journal and The New York Times, among many others.

PAUL KUBLER, CISSP, EnCE, CCNA, Sec+, ACE, is a digital forensics examiner at LIFARS. He’s a former employee at Boeing in the Global Network Architecture division and previously worked at the Flushing Bank in network and systems infrastructure, protecting valuable financial data at various levels within the network and systems. With several years of experience in cybersecurity and digital forensics, he conducted a wide range of investigations, including data breached through computer intrusions, theft of intellectual property, and computer hacking. Kubler has also performed forensic investigations into mobile devices, aiding in the prosecution of criminals. He belongs to several industry groups, including the Electronic Crime Task Force (ECTF), International Association for Computer Information Systems (IACIS), High Technology Crime Investigation Association (HTClA) and the Long Island Association of Information Technology Professionals (LI-AITP).

InfoSecurity Professional • 22 • May/June 2016
Join us for the Sixth Annual

SECURITY CONGRESS 2016

ADVANCING SECURITY LEADERS

Sept. 12 - 15 • Orlando, FL • Orange County Conv. Center

REGISTER NOW
For Early Bird Pricing Through July 31

Tracks include:
- Cloud Security
- Swiss Army Knife
- Professional Development
- Threats
- Forensics
- People Centric Security
- Application Security/Software Assurance
- Governance, Regulation and Compliance
- Incident Response
- Malware
- Mobile
- Threat Intelligence

This year earn up to 46 CPEs

Early Bird Pricing

4-Day (ISC)² Member: $895
4-Day Non-Member: $1,150

REGISTER TODAY
congress.isc2.org

#ISC2Congress

© Copyright 2016. (ISC)², Inc. All rights reserved.
The NICE Way to Address Cybersecurity Shortfalls

Education is one way to ensure there are enough qualified professionals to fill the information security pipeline in the coming decade. BY DOUGLAS MICHAEL RAUSCH

The search is on for qualified cybersecurity professionals. The often-cited (ISC)² Global Information Security Workforce Study (https://www.isc2cares.org/IndustryResearch/GISWS/) projects a 1.5 million person shortfall of qualified workers in just four years. That means by 2020, we will have more to do, more to protect within our organizations, and not enough qualified people to do it.

Unfortunately, as many private and public organizations have found, normal hiring channels are coming up short. The pool of qualified applicants is just not large enough to meet the need.

In response, the focus on workforce improvement programs has continued to grow. Programs to improve an organization’s existing workforce, establish undergraduate and graduate programs in cybersecurity, as well as plant the seeds of cyber careers in elementary, middle and high schools, have all begun to move forward with intensity.

These efforts were the centerpiece of discussion at last November’s National Initiative for Cybersecurity Education (NICE) Conference (http://csrc.nist.gov/nice/) in San Diego, which I attended. Academics, industry leaders and government officials reviewed evolving standards, current initiatives and ways to reduce workforce gaps.
Initiatives discussed at the NICE conference tended to fall into one of four focus areas: cybersecurity education and outreach in secondary education; post-secondary cybersecurity education; industry activities to acquire and improve the cybersecurity workforce; and government efforts to promote a formalized cybersecurity workforce. Space does not permit a session-by-session conference summary, but here are highlights of some of the many noteworthy activities.

The Bureau of Labor Statistics projects a 37 percent increase in the need for cybersecurity analysts from 2012 levels by 2022, according to a news article (www.upi.com/Top_News/US/2015/03/10/Cybersecurity-has-a-talent-shortage/3711425913442/) last year carried by the UPI wire service. The college graduates of 2022 are currently juniors in high school, which is a good age group to introduce career options to help fill that projected workforce gap. Current outreach includes the National Security Administration’s NSA Day of Cyber (www.nsadayofcyber.com) to provide students suggested education and experience paths to develop a cybersecurity career.

Additionally, the NSA and National Science Foundation are again sponsoring the GenCyber (www.gen-cyber.com) program this year, providing summer camp opportunities to students and teachers at the K-12 level. These camps, hosted by various organizations through GenCyber program grants, provide an environment for learning sound cybersecurity principles and teaching techniques.

A common problem discussed at the conference was how to classify workforce skills. Academic supply needs to meet industry demand, but that task is made more difficult when academia and industry do not use the same language to describe graduate skills and organizational and workforce needs.

The National Cybersecurity Workforce Framework (https://niccs.us-cert.gov) is showing some success as a lexicon of cyber workforce roles that everyone can agree upon. Changes to the U.S. Department of Defense workforce qualification standards were also of interest at the conference, with the existing DoD Directive 8570 being replaced with DoD Directive 8140 last summer. This directive begins the process of aligning the DoD cyber workforce qualifications with the National Cybersecurity Workforce Framework. To complete the transition, the accompanying DoD Manual 8140 must be published to replace the existing DoD Manual 8570, and that work is underway.

Rather than existing as four independent focus areas,
these activities must advance in an integrated manner. Secondary education must identify, cultivate and prepare our future cybersecurity workforce for a variety of post-secondary educational opportunities.

Our profession is maturing and growing more complex. We are closing in on the day when students will say they want to major in cybersecurity, just as they now say they want to major in engineering. An engineering student has many options within that field, such as studying to become a mechanical, electrical, civil or chemical engineer. In a similar manner, a cybersecurity student will look to specialize in incident response, forensics, risk management, or another area.

For now, let’s be grateful more students are choosing this path. Let’s also recognize that we as members can help strengthen our cybersecurity workforce and mentor students while they receive focused, hands-on education that can lead to an entry-level career path. In doing so, we all benefit.

DOUGLAS RAUSCH, CISSP, is director of the undergraduate cybersecurity studies program at Bellevue University in Nebraska and a cybersecurity consultant to government and commercial entities.

IN THE UNITED STATES
The President’s Computer Science for All
The president’s upcoming budget will include $4 billion in funding for states to increase access to computer science in P-12 classrooms during the next three years.

In addition to state-level grants, the budget will also dedicate $100 million in competitive grants specifically for leading districts to execute ambitious computer science expansion efforts for all students, including traditionally underrepresented students, and serve as models for national replication.

IN THE UNITED KINGDOM
Cybersecurity Principles and Learning Outcomes Guidelines
Some 20,000 future computer science undergraduates annually at 100 U.K. universities can now benefit from new higher education cybersecurity learning guidelines published by (ISC)² and the Council of Professors and Heads of Computing (http://cphc.ac.uk/). The guidelines are designed to better align academics with industry demands and reflect broad consultation with more than 30 universities and industry bodies and support the U.K. government’s National Cybersecurity Strategy. In those schools where the guidelines are implemented, students can be taught a broad spectrum of cybersecurity concepts, from threats and attacks to designing secure systems and products to governance based on up-to-date industry expertise.

NATIONS RESPOND TO THE SHORTAGE WITH FUNDS, CURRICULA UPDATES
(ISC)² Webinars

(ISC)² Webinars are developed to provide and help you earn CPE credits. These sessions are offered live, or even view the recorded sessions in the archives.

**e-Symposium**

Half-day online seminars that cover the latest topics top of mind with cybersecurity professionals around the world.

**ThinkTank**

Roundtable discussions that focus on the various industry and product verticals that exist within information security.

**Security Briefings**

Multi-part webinar that takes a “deep dive” into a topic by listening to the series over a short period of time.

**From the Trenches**

Roundtable webinar that features expert practitioners from different corners of the infosecurity world to discuss their “hands on” experiences in dealing with challenges and threats that are seen in their working day.
The Cat’s Almost Out of the Bag

Garfield is among many new additions to our cyber safety programs. **BY PAT CRAVEN**

**FEEL THAT BREEZE?** That’s coming from the staff and volunteers of the newly renamed Center for Cyber Safety and Education, who are running to work on their next revolutionary project. To date, we have launched our new website, www.SafeAndSecureOnline.org; released the groundbreaking Children’s Internet Usage Study; and, helped by the best cybersecurity professionals in the world—our members—we’ve redeveloped the ultimate parents’ educational program to keep their children and families safe when online.

It doesn’t stop there! One of the greatest things we get to do each year is award college scholarships to individuals who need a little extra help getting into the cybersecurity field. It is no surprise that the need is greater now than ever, evident by the record-breaking number of scholarship applications we’ve received. This year’s number of applicants far outpaces past years.

Thanks to great partners like Raytheon Company (http://www.raytheon.com), we are making a difference. Raytheon has made a three-year commitment with the creation of the Raytheon Women in Cyber Security Scholarship (http://www.raytheonlybercyber.com/news/feature/women_cyber_scholarship.html), which provides US$10,000 in assistance to two qualifying female students and includes a paid summer internship.

We also have creative initiatives in the works with partners such as Booz Allen Hamilton (http://www.boozallen.com), MITRE (http://www.mitre.org), the International Consortium of Minority Cybersecurity Professionals (ICMCP) (https://icmcp.org), O’Reilly Media (www.oreilly.com) and U.S. Cyber Challenge (USCC) (http://www.uscyberchallenge.org). Watch for more details on these partner initiatives soon.

This year, there will be several new fundraising events that you won’t want to miss, including a silent auction at this month’s CyberSecurGov and GISLA ceremony, along with a unique event at Security Congress in September that will emphasize the “fun” in fundraising.

That week, we will receive visits from two American icons: Garfield, the cat, and his creator, Jim Davis. Both will be on hand as we introduce Garfield as our new “spokescat” for our children’s version of Safe and Secure Online. At the event, we will unveil the first of a series of cartoons, modules and comic books in which Garfield and his friends teach children how to protect themselves online.

If all of that doesn’t have you spinning, keep in mind that later this year, you will also get the opportunity to contribute to the newly revised Global Information Security Workforce Study. This massive biennial effort attempts to capture the pulse of the cybersecurity industry and is widely cited by mass media for what it tells us about the state of the profession. Did you know that nearly 14,000 people participated in the last study? Such a large data set and historical references from years past make this a vastly anticipated study. You’ll want to be a part of it.

Can’t keep up with all of this? I suggest you sign up to receive regular updates on our new site, www.SafeAndSecureOnline.org, like us on Facebook (search SafeAndSecureOnline) and follow us on Twitter (@ISC2Cares). No matter what you do, hold onto your hat… because we are just getting started!
According to Certification Magazine's Annual Salary Survey, CCSP tops "The Next Big Thing" list as the #1 certification respondents plan to earn in 2016.

Is cloud security certification on your “to do” list?

As a CISSP, you have a special advantage over other candidates. You already meet the experience requirements and are immediately eligible to take the CCSP examination. These benefits* also apply to you:

» Free AMF – Pass the CCSP examination and your first year CCSP AMF is free
» Share CPEs – Your CPE requirements for CISSP count toward CCSP
» Discounted Instructor-led Training – US$1,400 for Classroom-based or US$1,100 for Live OnLine Training saving you US$850 off MSRP
» Special Pricing on Self-Study Tool – CCSP Training OnDemand is available for a special price of US$395

Download the Exam Outline

*(ISC)² reserves the right to change or cancel these promotions at any time without prior notice.
When you were a child, what did you want to be when you “grew up?”
I wanted to be a system programmer, like my father at that time. He always told me “not to worry, you will grow out of it.” Eventually, I did, and nowadays, we both work in IT security.

What changed that led you to become an information security professional?
During my university years as a computer science major, I took a few security-related courses. I liked them so much that I decided not to be a software engineer but to find a job in IT security instead.

What have been some of your biggest personal challenges in this career?
I think that my biggest challenge ever was finding my first full-time IT security job as a young professional without prior experience. Once I got over that initial obstacle, things became easier. From time to time, I have challenging tasks or projects, but I enjoy problem solving.

What are some of the biggest information security issues facing Hungarian organizations today?
Apart from the usual regulatory- and technology-related issues that are the same for everyone worldwide, Hungary is just beginning to implement stricter information security requirements for the public sector, while the financial sector and telcos already have a mature security environment in place. This transition requires people from very different backgrounds and organizations to cooperate, and sometimes it is quite difficult to reach a common understanding or share necessary information.

How has becoming a part of (ISC)² helped your career?
I consider getting the CISSP certification an important milestone in my career that has really helped me achieve my professional goals. Being an (ISC)² member and a local chapter official has also provided me great resources and opportunities to meet excellent colleagues.

There is often mention of the need for more women in security here in the USA. Is there also demand for more women in security in Hungary?
Yes. Employers are really looking for more professional women to hire, but to tell the truth, there is a huge demand (in general) for more qualified information security professionals in Hungary, so gender bias does not seem to be a big hiring issue now.

What do you think can be done to bring more women and other underrepresented minorities into the profession?
I believe that investing in education and creating equal opportunities for young people, regardless of gender or any other consideration not related to their abilities, are very important. We have some great local initiatives, and I am personally involved in WITSEC (Women in IT Security), an organization that offers mentoring to young professionals by women with established careers in information and IT security.

What do you like to do to relax during your time away from work?
I belly dance for fun. It is so different from what I do for work that it can completely take my mind off even the most nagging professional problem.

If you could recommend one place everyone should visit at least once in their lifetime, what would it be, and why?
There are many beautiful places around the world, but for me, the dearest place for summer holidays is Lake Balaton, which is the largest lake in Central Europe. It is quite shallow, and during the summer, the water gets quite warm. During sunset, the wind usually stops, and the water is very still. It turns golden, then silver, while the sun disappears behind the hills. I love swimming in the lake at that time.
At Twirling Tiger Media, our dedicated editorial and graphics team can create relevant and valuable content that engages and nurtures your target audience and puts you center stage as a solution to their challenges.

From concept to deliverables, we are your one-source content solution.

Our content creation capabilities include:
- Articles
- Blogs
- Case Studies
- Content Marketing
- Content Strategy
- Custom Content
- Digital Media
- eBooks
- Infographics
- Inspirational Quotes
- Leadership Guides
- Marketing Collateral
- Press Releases
- Publications
- RFPs and Proposals
- SEO Copy
- Success Stories
- Web Content
- White Papers and more!

Contact Bob Ostrow today at bostrow@twirlingtigermedia.com
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