SECURITY ACCOUNTABILITY IS EVERYONE’S JOB

TIPS ON BUILDING A CHAMPIONSHIP-WORTHY CYBERSECURITY TEAM
SECURITY’S ROLE IN AGILE SOFTWARE DEVELOPMENT

also

A WORD FROM A LONGTIME CISSP
HOW TO CREATE GOALS TO INSPIRE YOUR TEAM
5 MINUTES WITH MARY N. CHANEY
ISHPI is honored to sponsor Dr. Peter W. Singer, an iconic Author, Visionary and Cyber Warfare Strategist, as a Speaker and signing Author. Dr. Singer has been dubbed “one of the ten most influential voices in the world on cybersecurity.” He will present his thoughts on: “NextWar: The Future of Technology and Geopolitics”

Monday, September 12: 11:00 AM - 12:00 PM

Dr. Singer will be signing his books at the (ISC)^2 book store,
Monday, September 12: 2:45 PM - 3:15 PM

Join us at our sponsored event

Exclusive Member Networking Celebration
The (ISC)^2 Member & Attendee Party offers a great opportunity to network with other (ISC)^2 members and full conference attendees
September 13, 6-9 p.m. @ Kings Bowling

ISHPI is the exclusive Sponsor of the:
Speaker Reception

Girish Seshagiri
VP | CTO at ISHPI
Will also be a Speaker at the Security Congress

Girish will share his thoughts and insights on one of the hottest topics in the Cyber/Software industry: “Agile teams and high maturity practices create secure software”

Wednesday, September 14: 11:00 AM - 12:00 PM

About ISHPI

ISHPI works in concert with other defenders of the Homeland to fortify national preparedness, agility, strength and advantage in the cyber domain. Our Information Operations group, our CMMI Dev/5 appraised Advanced Information Services group, our C5ISR Engineering & Technical Services group, and our (ISC)^2 OTP Training & Consulting business groups work in unison to provide experienced people, proven processes, technology, advice and leadership to enable full spectrum Cyber capability.
FEATURES

› MANAGEMENT

18 All In
To move from security awareness to security accountability takes a commitment from everyone—from the back room to the boardroom.
BY SHAWNA McLEARNEY

› MANAGEMENT

22 Building a Championship-Worthy Team
Putting together a successful cybersecurity staff requires finding (and recruiting) the right combination of people and skills.
BY DEBORAH JOHNSON

› Q&A

26 Talking Cybersecurity with Two Cool Cats
Jim Davis and his cartoon creation, Garfield, discuss art, activism and promoting Safe and Secure Online.
EDITED BY ANNE SAITA

› TECHNOLOGY

28 ‘Why Johnny Can’t Write Secure Code’
Understanding today’s agile software development can help make security a bigger part of the application development process.
BY KEITH McMILLAN

Cover image: JOHN KUCZALA. “Garfield” Character(s): ©PAWS. All Rights Reserved. Image (above): PETER AND MARIA HOEY.
HOW DO YOU RATE?

ILL WHERE YOU WORK someday depend on a company’s cybersecurity score?

Fair Isaac Corp., better known as FICO, this summer announced it will start offering enterprise-level cyber risk security scoring after acquiring startup QuadMetrics, which uses predictive analytics to determine an organization’s cybersecurity posture.

“Just as the FICO score gave credit markets a single metric for understanding credit risk, this product will give the industry a common view of enterprise cybersecurity risk,” said FICO VP of cybersecurity solutions Doug Clare in a prepared statement. The company expects its new FICO Enterprise Security Score to assist cyber insurance policy underwriters and others in determining the risks of working with a specific company or third-party vendor.

Any consumer who has applied for credit knows the power of FICO scores. A high score can qualify you for a better mortgage or auto loan. Similarly, a low score can limit not just purchases but where you live and even work. Those with a longer history of managing credit will have an advantage over those just starting out.

In the business world, the new FICO scores could not only influence who gets the deal but at what price. Surely a company with a high cybersecurity rating has more negotiating power than one that doesn’t. Security professionals also may be able to boast in job interviews about an employer’s rising scores (perhaps in general terms if the scores are confidential), while those working at low scorers risk being laid off resulting from a loss of business.

Those who’ve been demanding more resources might be able to use the new FICO score to gain buy-in. After all, executives still stumped by the security dashboards they currently receive can grasp these scores, even if they don’t understand the algorithms behind them.

Finally, let’s not forget that a high FICO Enterprise Security Scoring company doesn’t mean cyber criminals can’t break into its networks. It just means the digital underground may have to work harder to find where the company is vulnerable.

—ANNE SAITA  asaita@isc2.org

ADVERTISER INDEX

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

Ishpi .................................................. 2
Capella University .................................. 5
TechTarget ........................................ 7
(ISC)² .................................................. 9
(ISC)² .................................................. 11-14
(ISC)² .................................................. 15
Intel .................................................... 17
Executive Women’s Forum ..................... 21
Sunera .............................................. 25
Rackspace ........................................ 31
Twirling Tiger Media ............................ 35
(ISC)² .................................................. 36
(ISC)² .................................................. 37

(ISC)² MANAGEMENT TEAM
 SENIOR MANAGER, MEMBERSHIP MARKETING AND MEDIA SERVICES
 Jessica Hardy
 727-785-0189 x4063
 jhardy@isc2.org
 EXECUTIVE PUBLISHER
 Timothy Garon
 508-529-6103
tgaron@isc2.org
 MANAGER, GLOBAL COMMUNICATIONS
 Amanda D’Alessandro
 727-785-0189 x4021
 adallessandro@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
 Carlos Canoto South America
 Amanda D’Alessandro (ISC)²
 Tushar Gokhale U.S.A.
 Javvad Malik EMEA
 J.J. Thompson U.S.A.
 Elise Yacobelli (ISC)²
 TWIRLING TIGER MEDIA
 EDITORIAL TEAM
 EDITOR-IN-CHIEF
 Anne Saita
 asaita@isc2.org
 ART DIRECTOR & PRODUCTION
 Maureen Joyce
 mjoyce@isc2.org
 MANAGING EDITOR
 Deborah Johnson
 MEDIA SERVICES COORDINATOR
 Amanda D’Alessandro
 727-785-0189 x4021
adalessandro@isc2.org
 COMMUNICATIONS MANAGER, GLOBAL
 Timothy Garon
 508-529-6103
 Tim Garon
 EXECUTIVE PUBLISHER
 Jessica Hardy
 727-785-0189 x4063
 jhardy@isc2.org
 AND MEDIA SERVICES MANAGER
 Jennifer Hunt
 781-685-4667
 jhunt@isc2.org
 EVENT SALES MANAGER
 Lisa O’Connell
 781-460-2105
 loconnell@isc2.org
 COMMUNICATIONS MANAGER, GLOBAL
 Timothy Garon
 508-529-6103
 Tim Garon
 EXECUTIVE PUBLISHER
 Jessica Hardy
 727-785-0189 x4063
 jhardy@isc2.org
 AND MEDIA SERVICES MANAGER
 Jennifer Hunt
 781-685-4667
 jhunt@isc2.org
 EVENT SALES MANAGER
 Lisa O’Connell
 781-460-2105
 loconnell@isc2.org

Ishpi .................................................. 2
Capella University .................................. 5
TechTarget ........................................ 7
(ISC)² .................................................. 9
(ISC)² .................................................. 11-14
(ISC)² .................................................. 15
Intel .................................................... 17
Executive Women’s Forum ..................... 21
(ISC)² .................................................. 25
Sunera .............................................. 30
Rackspace ........................................ 31
Twirling Tiger Media ............................ 35
(ISC)² .................................................. 36
(ISC)² .................................................. 37

Twirling Tiger Media is certified as a women’s business enterprise by the
ternational Council (WBENC).
This partnership reflects (ISC)²’s commitment
to supplier diversity.
www.twirlingtigermedia.com

©Rob Andrew Photography

Editor’s Note

Anne Saita, editor-in-chief, lives and works in Southern California.
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
Fifteen years ago, I boarded a train bound for Washington, D.C., to spend a long, long day taking the CISSP exam. With no official exam preparation books, my own prep came from reading the “blue book” from cover to cover. The test was paper-based, and I remember some last-minute shopping for No. 2 pencils. I also remember being the youngest person in the exam room that day.

It was a taxing day, but a few months later, I received a letter that I’d passed the exam. The CISSP was my first professional certification and the only one I’ve kept over the years.

Getting that (ISC)² certification helped me advance in the IT security job I held at the time, and it definitely played a role in helping me get my next job. Since then, I’ve held numerous positions at different companies, including my product management role on the Security & Privacy team at Google today. Just as my career has grown and shifted direction over time, so, too, has (ISC)² evolved from a certification body into a membership organization. Over time, I realized I wanted to play a more active role in guiding the organization and the independent 501(c)3 charity known as the Center for Cyber Safety and Education.

We as a board want to ensure that you continue to have access to the resources you need to stay competitive and competent as threats evolve and business demands increase. We also hope that we, as a membership, invest not only in our own careers, but raise the bar for the cybersecurity industry and the greater communities we serve. This is one reason I’m so committed to the work begin done at the Center for Cyber Safety and Education.

We as a board want to ensure that you continue to have access to the resources you need to stay competitive and competent as threats evolve and business demands increase. We also hope that we, as a membership, invest not only in our own careers, but raise the bar for the cybersecurity industry and the greater communities we serve. This is one reason I’m so committed to the work begin done at the Center for Cyber Safety and Education, the charitable organization affiliated with (but independent from) (ISC)².

If you’ve ever wanted to “give back” to the industry and make the world a better, safer place, now is your chance. The Center offers many opportunities for you to share your expertise and is expanding programs in all three of its core areas: education, research and outreach.

- In the education area, the Center has been seeing record numbers of scholarship applicants, and we are excited to be able to help the next generation of cybersecurity professionals get access to the education and internship opportunities they need to meet the rising demand for cybersecurity professionals.
- In research, the eighth Global Information Security Workforce Study, the canonical source of information on the IT security workforce, has been open for a few weeks at the time of this writing. So far, the number and distribution of respondents is strong. The Center is also exploring additional types of research that can further its mission to ensure a safe and secure cyber world.
- In outreach, the Center has radically revamped Safe and Secure Online, its banner program, to improve our ability to reach kids, parents and educators. This includes the introduction of a new “spokescat,” Garfield, whom we hope will help cyber safety awareness become second nature for people worldwide.

You can learn more about all of these programs, including how to get involved, by checking out isc2cares.org.

As we grow and advance in our careers, it’s only natural that our relationship and involvement with a membership organization like (ISC)² is going to change. Maybe you joined simply to get a certification to qualify you for a specific job. Or, perhaps you took some courses just to understand the scope of IT security.

In any case, the board and management want to see you succeed. We also want to know, whether at this month’s Congress conference, or through conventional communications channels, what you need from a professional organization today, and, perhaps more important, tomorrow.
Identifying and Neutralizing Cyber Threats

Threats don’t just lay in wait
In fact, they’re actively assaulting your systems right now

63%
of IT and security professionals experienced at least 1 breach resulting in data loss over the past 24 months*

*According to a recent SANS Institute study

Win this battle with the help of security experts

Could you better protect your network against a breach by taking a more holistic view on security? Find out inside

This three-part guide explains the latest means for rooting out the fast-moving malicious actors that are targeting your enterprise systems

Which 3 strategies can help you find enterprise shadow cloud usage? Learn all 3, plus how cloud threat modeling differs from traditional methods

Get your 3 free e-guides today in less than 2 minutes at: www.SearchSecurity.com/ISC2Security
(ISC)² Community Choice Winners Recognized at Middle East Security Awards

(ISC)² received a special honor for its Outstanding Contribution to Information Security in the Middle East during the first Middle East Security Awards (MESA) CISO 100 and (ISC)² Community Choice Awards. Spearheaded by the United Arab Emirates (UAE)-based CISO Council, (ISC)² accepted the award at a gala during the Middle East Security Awards Conference last May.

The (ISC)² Community Choice Awards complemented the juried CISO 100 honorees by giving practicing members the opportunity to vote on and recognize industry leaders from within their community. The following (ISC)² Community Choice Award winners, presented by Faisal Malik (pictured below), head of business and market development (EMEA), have played a formative role in the fast-maturing capacity for cybersecurity in the Middle East:

(ISC)² MESA Woman Security Leader: Fatma Bazargan, CISSP, CISO, Injazat Data Systems

"It is a real privilege to win this award. When I returned to work, my CEO had sent a note out to the entire office," says Fatma Bazargan.

In her role, Bazargan acts as a CISO for technology service provider Injazat. Interaction with firewalls while studying for her undergraduate degree in computer engineering helped her discover a passion for information security. She traveled to the United Kingdom to pursue a master's degree in computer systems security at the University of Glamorgan and returned to an opportunity to work at the Telecommunications Regulatory Authority (TRA) as a network security engineer. This was a formative stage for information security, which presented Bazargan the opportunity to help found a national incident response center, AE-CERT, a project that she went on to lead and later manage. She then took on the challenge of building the master security program for Masdar City—a unique endeavor to create a world-first ecologically sustainable city in Abu Dhabi.

Bazargan, the first woman in the UAE to become a Certified Information Systems Security Professional (CISSP), notes her drive to pursue education as a woman in the field. She has a Ph.D. in computing engineering, is qualified as an ISO 27001 lead auditor, and this fall will enter Carnegie Mellon University's CISO Executive Program.

(ISC)² MESA Government Security Leader: Abdulla Al Sayari, CISSP, CISO, Abu Dhabi Health Authority

Abdulla Al Sayari has worked in information security for seven years, stepping into his first role after completing a bachelor's degree in information security from United Arab Emirates University. He has developed a reputation for achieving results, which has earned him such awards as Young Government IT Professional of 2016, before being included in the CISO 100 and chosen for the Community Choice Award.

Al Sayari led an ambitious program to establish information security as an independent unit within the Abu Dhabi Health Authority, establishing a new corporate security policy to communicate well-understood standards for both the authority and the health care companies it regulates. Expected to take five years to launch, the new unit is now established and delivering clear benefits within the three years that Al Sayari has been in his role. “Our objective is to motivate a real cultural shift in the organization, not just the transformation of processes,” he explains.

Al Sayari involved business owners as well as IT teams in the management of issues, which paved the way toward the desired cultural shift.

(ISC)² MESA Information Security Leader: Sarfaraz Kazi, CISSP, Infrastructure Security Manager, National Bank of Kuwait

Sarfaraz Kazi leads major infrastructure projects in NBK's Information Security Office and aligns systems to meet compliance requirements.

"Receiving the leader award was a great feeling. I was not expecting it, as there were so many other experienced information security professionals around me on the night," he says.
Originally from Mumbai, India, where he began his career in IT, Kazi was encouraged by stories of career opportunities to join family members living in Kuwait 15 years ago. With a network security background, he became a CISSP in 2010, which he counts today as a watershed moment in his career. “This is when doors really started to open for me. I realized just how big the information security professional domain was, which completely changed the way I communicated with colleagues and changed how I was able to develop my career,” he says.

Kazi soon became an active volunteer for (ISC)² and the development of the professional community in Kuwait. He became an exam proctor, an adviser, and in 2012 founded the first (ISC)² chapter in the Gulf Region, in Kuwait. Today, the chapter hosts four education events for the Kuwait security community a year, which always attract good sponsorship and has become respected as a forum for cross-industry information sharing. Kazi remains involved as chapter secretary, but the leadership has been successfully passed on to other chapter members.

CPEs
Please note that (ISC)² submits CPEs for (ISC)²’s InfoSecurity Professional magazine on your behalf within five business days. This will automatically assign you two Group A CPEs.

(ISC)²® ANNOUNCES
2016 ASIA-PACIFIC INFORMATION SECURITY LEADERSHIP ACHIEVEMENTS (ISLA) HONOREES

This summer, (ISC)² honored 35 information security professionals and four workforce initiatives during its 10th annual Asia-Pacific Information Security Leadership Achievements (ISLA) Program. A ceremony occurred July 26 at Centara Grand at CentralWorld, Bangkok, Thailand. Concurrently, (ISC)² Security Congress APAC, co-hosted with the Electronic Transactions Development Agency (ETDA) and the Ministry of Information and Communication Technology (MICT) of Thailand, in partnership with Image Engine Pte. Ltd., took place at the same venue.

“This year, we received many top-notch nominations from the entire Asia-Pacific region. We believe that many in the industry support the mission of Asia-Pacific ISLA to commend the great work of the heroes and heroines in this industry,” said (ISC)² CEO David Shearer.

The 2016 honorees are as follows:

Information security practitioner category:
- Kai Chi Chang, Section Head of Network Security Data, National Center for Cyber Security Technology & Institute for Information Industry (Taiwan)
- Joyce Fan, CISSP, CSSLP, Vice Chairperson (Membership & Constitution), Professional Information Security Association (Hong Kong)
- Kosetsu Kayama, CISSP, Cyber Defense Center Manager, Fujitsu Limited (Japan)
- Kyu-ho Lee, CTO, Secuve Co., Ltd. (Korea)
- Wayne Wei-Wen Liu, CISSP, CISA, CGEIT, Senior Information Security Manager, Advanced Semiconductor Manufacturing Co., Ltd. (China)
- Vijay Luiz, CISSP, CISA, Secretary, (ISC)² Singapore Chapter (Singapore)
- Dr. Ching-Hao Mao, CCJK, OCPJWCD, SCJP, Section Manager, Institute for Information Industry (Taiwan)
- Moshiri Islam Mishu, CISSP, CISA, CFIE, Security Engineer, Augmedix (Bangladesh)
- Phannarith Ou, Director of ICT Security, Ministry of Posts and Telecommunications (Cambodia)
- Syed Zafar Saeed, CISSP, CISA, CISM, IT Security Architect, Avaya (India)
- Jumpon Suwanphahu, CISSLP, SSCP, Security+, Consultant, ACIS Professional Center Co., Ltd. (Thailand)
- Tony Tsai, LPI Level 1, Encase I/II, ISO/IEC 17025, Manager of Digital Forensics Center, Acer CyberCenter Services, Inc. (Taiwan)

Information security educator category:
- Rabat Lakmal Rupasinghe, MBA, CISSP, CISA, Senior Lecturer/Consultant, SLIIT (Sri Lanka)

Senior information security professional category:
- Dongkeun Choi, Director, CISO, CPO, LOTTE Card Co., Ltd. (Korea)
- Shin-ichi Fuchigami, CISSP, SSCP, CCAI, Vice President, International Information Technology Business College (Japan)
- Chen-che Hsu, Engineer, Chunghwa Telecom (Taiwan)
- Albert Hui, GXPN, GREM, CRISC, Principal Consultant, Security Ronin (Hong Kong)
- Dr. Mingu Jumaan, B.Sc., M.Sc., Ph.D., Director, Sabah State Computer Services Department (Malaysia)
- Hisashi Kasahara, CISSP, ISSAP, Manager, NEC Management Partner, Ltd. (Japan)
- Chan Lee, CISSP, CISO, CTO, CTO, Secuve Co., Ltd. (Korea)
- Otto Lee, CISSP, CSSLP, CISA, Chairperson, Professional Information Security Association (Hong Kong)
- Anthony Lim, CISSP, CSSLP, Manager, Senior Cybersecurity Adviser, Asia-Pacific, Frost & Sullivan (Singapore)
- Indranil Mukherjee, CISSP, ISO 27001:2013 Lead Auditor, CISA, Managing Director, Singapore ISC Pte. Ltd./ISC Global (Singapore)
- Todorovic Vladan, M.Sc., Founder, Advanced Security Technologies Asia Pte. Ltd. (Singapore)
- King Cheung Kelvin Wong, Officer, Hong Kong Police Force (Hong Kong)

Managerial professional for information security project(s) category:
- Raul Paolo Miranda, CISSP, CITPM, Master’s in CIO Practices, Membership Director, (ISC)² Singapore Chapter (Singapore)
- Seungwoo Nam, CISSP, CISO/CPO, NH Bank (Korea)
- Kumpol Sontanarat, Director of ICT Department, Securities and Exchange Commission (Thailand)
- Victor Yeo, CISSP, QISP, Deputy General Manager, ST Electronics (Infosecurity) Pte. Ltd. (Singapore)
- Suk Jin Yun, Partner, EY Han Young (Korea)

Information security educator category:
- Dato Dr. Norbik B. Idris, Professor, Universiti Teknologi Malaysia (Malaysia)
- Dr. Heejo Lee, Professor, Korea University (Korea)
- Hung Leung, Senior Lecturer, Hong Kong Institute of Vocational Education (Chai Wan) (Hong Kong)
- Prabath Lakmal Rupasinghe, MBA, CISSP, CISA, Senior Lecturer/Consultant, SLIIT (Sri Lanka) ©
(ISC)² Congratulates all 2016 finalists!

The Americas ISLA Program recognizes information security and management professionals throughout the private and public sectors in North, Central and South America, with the exception of the U.S. federal government (recognized through the GISLA Program), for their outstanding leadership and achievements in workforce improvement.

Categories:

» Senior Information Security Professional
» Information Security Practitioner
» Up-and-Coming Information Security Professional
» Community Awareness

Location:
September 14, 2016
Jimmy Buffett’s Margaritaville
Orlando, FL
2016 Finalists

Senior Information Security Professional

Diego Andres Zuluaga Urrea
Project/Initiative: Leadership of the Colombian Energy Sector Cybersecurity Improvement

Bently Au, CISSP
Project/Initiative: Enterprise Information Security Program for Toyota Motor Sales, USA, Inc.

Dr. Eric Cole
Project/Initiative: Detection of Computer System Intruder Access

Information Security Practitioner

Mack Bhatia
Project/Initiative: Enterprise Integration - SOC 2 and SOC 3 compliance

Marco Tulio Oliveira de Moraes, CISSP
Project/Initiative: Information Security Practitioner Web Security
Up-and-Coming Information Security Professional

Jennifer Chermoshnyuk
Project/Initiative: CLE (Continuing Legal Education) Program

Edward Skaife, CEH, CPT
Project/Initiative: Cybersecurity Solutions at Forward Health Group, Inc.

Community Awareness

Deidre Diamond
Project/Initiative: Hang Together

Sandra Toner
Project/Initiative: Online Cybersecurity Awareness Tools
Thank You to the Judging Committee

Gerardo Castillo, CISSP
IT Infrastructure Manager for Latin America, National Instruments Costa Rica
(ISC)² Latin American Advisory Council Member

Geraldo Fonseca, CISSP
Corporate Information Security Officer, ONS
(ISC)² Latin America Advisory Council Member

Jefferson Gutierrez, CISSP
Managing Director, Forensic Services
(ISC)² Latin American Advisory Council Member

Gurdeep Kaur, CISSP
Chief Security Architect, AIG
(ISC)² North American Advisory Council Member

Glenn Leifheit, CISSP, CSSLP
Senior Security Service Architect at Microsoft
(ISC)² North American Advisory Council Member

Marie E. Olson, CIPM, CIPP, CISM, CISSP
Deputy Chief Privacy Officer, Global Privacy Office, The Boeing Company
(ISC)² North American Advisory Council Member

Ramiro Rodrigues, CISSP, CISM, CICISO, PMP, MsC
Chief Information Security Officer at Serasa Experian
(ISC)² Latin American Advisory Council Member
InfoSecurity Professional Magazine Wins Bronze Award in International Competition

Competing in a field of more than 400 entries for a 2016 Tabbie Award, art director Maureen Joyce, along with photo illustrator John Kuczala and our editorial staff teamed up to create an award-winning entry in the Front Cover/Digital Imagery category. The Tabbie Awards are an annual competition created by the Trade Association Business Publications International (TABPI) and recognize excellence in B2B editorial and design. The judging comments stated, “Interesting concept that is well played out. Good use of fonts and colors.”

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

https://www.globalknowledge.com

$104,949

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.

The average salary for an IT security professional last year, making it the third best paying job in IT, according to a 2016 Global Knowledge survey.
How to Create Goals That Get Your Team Excited

BY KASHIF IQBAL

I RECALL ONCE managing a team of network and security professionals. When it came time to set goals, one of the senior engineers wrote this comment: “Why bother? No one in the team takes it seriously, and it is just a tick-box exercise.”

By then, I’d been managing that team for five months and surprisingly found myself privately agreeing with the frustrated engineer, who had the courage to say what I suspect everyone else was thinking.

So, I went back to my company’s HR team and my director and confidentially asked to delay the team’s required goal-setting activity for three more months. During that time, I focused on discovering what each team member cared about. I even invited the entire team to talk about their aspirations and motivations over drinks at my favorite bar.

In short, I discovered what made each team member “tick” so that we could achieve something together that, well, meant something to each of us.

Setting up team goals is a challenging task, especially compared to setting up your individual goals. You cannot set a team’s goals and believe you will get there without first considering each member’s strengths and weaknesses and effectively communicating what success looks like.

Consider asking yourself the following three P’s:

**Purpose:** Why does my team exist? What value does my team add to the business? What does my team need to achieve, and what are the implications if my team doesn’t achieve it?

**Process:** How will my team achieve this goal? What skills and resources do we need to get there?

**Performance:** What are my targets? Key performance indicators?

Once you get all these sorted, you should sit down with individual team members and together decide on a goal—and the steps to achieve it—that touches on some of the following...
Top Reasons to Attend the FOCUS 16 Intel® Security Conference

November 1-3 in Las Vegas | ARIA Resort and Casino

Hear Special Guest Keynotes Ashton Kutcher & Ted Koppel

Engage With Our Leaders

Anticipate The Next Threat with McAfee® Labs

Build Your Arsenal with Case Study Successes

The Market Dynamics of Cybersecurity

Save $100. As an ISC2 member, you can save $100 off your registration by using promo code FOCUS16 when registering!

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation.

To learn more visit us at focus.intelsecurity.com/Focus2016

---

key points:

- Performance (the what)
- Timeline
- Process (the how)
- Purpose (the why)
- Individual (what inspires each person on the team?)
- Measurement (quantity or quality)

To help illustrate how you can incorporate these key points into a formal goal, here’s an example:

In order to better accommodate an increasingly mobile workforce, our team will develop the very first digital hospital transformation program by building a robust, flexible and more mobile-friendly wireless network. We’ll collaborate with A&E staff and utilize our vendor’s gold partnership in order to have the advanced wireless network up and running by the end of the financial year.

The above recommendations are similar to establishing SMART (specific, measurable, attainable, relevant and timely) goals. Based on my own experiences managing teams, I recommend the following tips to set goals that your team members not only want to achieve but will.

- Goal-setting is more than a yearly activity; keep the goals alive.
- Celebrate past successes.
- Restructure team goals so that they are personal and matter to individuals.
- A good goal includes an expectation and articulates the process for achieving it.
- Make sure a goal is not too much of a stretch for the individual. Remember, you want to build each team member’s confidence.

Remember also that most goals are not static; therefore, they may need a refresh as things change.
CONGRATULATIONS! You and your security team finally have greater awareness of security issues and best practices at your company. But, you’re only halfway there. After companywide awareness, you need everyone to be responsible for keeping the company safe from cyber criminals. This includes everyone in the organization, most of whom do not report to you.

“We need to move from the status quo and involve security in a manner that holds everyone accountable,” says David A. Cruz, an information security and assurance expert with 10 years of experience helping organizations enhance their security programs. He currently is writing a book for business executives scheduled to be published later this year.

“Executives must lead this effort and hold themselves accountable for the actions, or lack thereof. It is no longer acceptable for one department or person to be operationally and functionally responsible for the security of an organization. Every business unit must share responsibilities and accountabilities when it comes to information security.

“The policy must reflect the same principles of accountability organizationally. The leader is responsible for instituting a policy that is enforceable,” adds Cruz, a Center for Cyber Safety and Education Safe and Secure Online program.
instructor and a professor at ITT Technical Institute. He’s implemented enterprise-wide security awareness and education programs and conducted hundreds of assessments associated with various industry standards for some of the largest financial institutions.

“The policy must clearly outline roles, responsibilities and the consequences for failure to meet the underlined expectations.”

ACCOUNTABILITY 101

“Accountability represents taking ownership of something and understanding the consequences,” says Pamela Fusco, the chief financial officer of the ISSA International board and an executive board member for several industry alliances. “When added to a training program, it literally transforms the trainee from a passive learner to an active learner, as they become individually and collectively accountable for the information that is being presented.”

She suggests that any relevant training programs today be interactive, with the participants demonstrating their competency and understanding. “It’s the ‘sticky bit’ that melds the paradigm between responsible use, activity and management of information for the business.”

FORMING YOUR ‘TEAM’

Consider that your “team” in this case is not only composed of those you manage but those at various levels who will support your efforts throughout the company. Look beyond what most security people would view as necessary and desirable for such a team.

“Chief is the buy-in from the CEO, as well as from all of the chief executives,” says Brett Osborne, chief information security officer at the Broward County Clerk of Courts office in Florida. “I created a board for Governance, Risk and Compliance made up of all the chief directors from HR, finance, business units, audit and legal.”

Osborne feels his GRC board is one of the most important aspects of his security awareness and accountability plan because its main focus is on all forms of risk (audit risk, legal risk, IT risk, information risk at the business unit level and reputational risk), and it involves and informs all of the disciplines.

Cruz agrees that one of the most important elements of an effective program is collaboration. “I worked with various department leaders from training, communications, marketing, HR, legal and other units to ensure this effort had the right components.

“I developed the content of the program, while the training department designed the structure. Communications wrote the message tailored for the intended audiences, and marketing formulated branding activities. Human resources developed procedures associated with disciplinary actions. Lastly, legal ensured that the policy contains the appropriate language to be legally enforceable. In conclusion, without legal’s and HR’s support, there is no accountability.”

GETTING THE NECESSARY BUY-IN

It makes sense to involve these department leaders, and with the CEO’s support, the program will mostly come together. But when looking at busy schedules, competing priorities, etc., how do you make security the winner?

Develop a good relationship with all of the directors. It’s a lot easier to grab a coffee with someone for a friendly request than to arrange a meeting. It can even work for staffing issues. As Osborne says, “I am the only security guy, so I have to delegate a lot to IT managers, network managers, and the help desk. Part of that is authorized by the CIO, but part of that is building the relationships.”

And helping them realize that it’s not just an IT issue but a business issue.

“Be independent—focus on information security. The business is the information owner, not the technology side,” says Osborne, who will be a presenter at the (ISC)² Security Congress 2016 in Orlando. “Security is more than IT, so you must reach out to the business side for input.”

Make your security program interesting and worthy of the time it takes to participate. Fusco, who has served on the U.S. Presidential White House Inaugural Staff and held positions as chief security strategist, chief information security officer and chief security officer for several Fortune 500 companies, offers several suggestions for capturing employees’ interests:

“when added to a training program, it literally transforms the trainee from a passive learner to an active learner, as they become individually and collectively accountable for the information that is being presented.”

—PAMELA FUSCO, chief financial officer, ISSA International board
Create an internal corporate video featuring staff members as villains and heroes. This has proven time and again to be one of the best “sticky bits” for security awareness training. When you portray the HR generalist as the “black hat hacker” and the CFO as the victim, with your security operations gurus hacker-tracking the activity, it becomes worthy of a town hall meeting for the entire corporation—popcorn and all.

Consider rubberneckers. Just about everyone slows down to see what’s going on when there are flashing lights on the highway. The same is true when you conduct a live hacking demonstration.

Make it personal. There is no doubt security training can be rather bleak. Integrating security knowledge that is specific to day-to-day activity is of interest to most of us. Doing a segment on the internet of things, detailing how an employee’s home security system is connected to his iPhone, which could impact the personal safety of his family or his ability to watch HBO, is fascinating and lays the foundation for a broader interest in security.

THE GATEKEEPERS
Everyone in the organization plays a role in security, but ultimately, leadership is accountable for protecting the brand.

“With this notion, they need to develop and promote a culture of accountability supported by legal and human resources in order to be enforceable,” Cruz says. “The policy ought to contain specific accountability clauses, and it must clearly define any disciplinary action intended to be taken when a violation occurs. The policy must have senior management support, and the accountability has to start at the executive level.”

When executives shift security accountability to their managers, it lessens its importance to the organization. “Managers, therefore, are unable to hold individuals accountable,” Cruz adds. “The decision-makers must be clearly and actively engaged in security. They must promote a security-conscious culture where everyone is responsible for security, from the back room to the boardroom.”

THE MUST-HAVES
When moving into security accountability, several key factors are vital to the success of the program:

- Management must lead by example and set an effective enterprise policy that consistently directs the behavior of the entire organization.
- Incorporate security into all business functions, i.e., a normal activity in which everyone at all levels protects the information entrusted to them.
- Establish a true culture of accountability, one where each person understands his or her individual responsibility and the consequences of failure. Couple that with a channel that permits everyone to contribute suggestions and identify potential security concerns.
- Integrate as much automation as possible. Self-service technologies and programs can reduce the resources required to support many programs.
- Be practical with your security program. Overly rigorous security requirements could cause your users to do the opposite of what you seek.

Information is the most pervasive element of an organization, and everyone at every level works with it in one way or another. In the end, business leaders must examine their risk tolerance, define an acceptable level of risk, and make sure every employee understands his or her obligations and is held accountable.

Securing such information is the responsibility of every division in the organization, as well as of each individual. Incorporating it naturally into all business functions will make it far less likely that your organization will be ridiculed on the evening news as a victim of the latest breach.

Remember, “Training doesn’t make users faultless,” Fusco says. “Training will, however, reduce the bloopers users make, which ultimately strengthens awareness, subdues business risks, reduces unexpected resource allocations—both financial and human resources—and enhances business.”

SHAWNA McALEARNEY is a freelance writer in Massachusetts and previous contributor to InfoSecurity Professional.
14th Annual

BALANCING RISK AND OPPORTUNITY:
Join your peers and learn to transform cybersecurity, risk and privacy beyond the enterprise.

Keynotes:
- Nina Burleigh, National Correspondent, Newsweek
- Susan C. Keating, President and Chief Executive Officer, National Foundation for Credit Counseling
- Meg McCarthy, EVP Operations and Technology, Aetna
- Valerie Plame, Former Operations Officer of the United States CIA
- Zoe Strickland, Global Chief Privacy Officer, JPMorgan Chase

Panels Include:
- Visualizing Security Analytics So Managers Can Understand & Act
- The Breaches We Know About; The Breaches We Don’t
- Behavior Analytics, Insider Threat & Employee Privacy Rights

October 25th
9:30am to 11:30am
Pre-Conference Leadership Journey Program
Join us for an optional 2 hour program to understand how conversation triggers different parts of your brain. Learn how to develop conversational skills that will strengthen the relationships that matter the most to you and can propel you toward greater success.

For more information on the EWF or to register, please visit: www.ewf-usa.com

Invest in Yourself!
ROI

EARN UP TO 19 CPE CREDITS
BUILD A NETWORK OF THE MOST DYNAMIC WOMEN IN OUR INDUSTRY
TAKE HOME TOOLS, BEST PRACTICES & SOLUTIONS TO ACHIEVE SUCCESS

October 25-27, 2016
Hyatt Regency at Gainey Ranch | Scottsdale, AZ

OVER 25 SESSIONS THIS YEAR!
BREAKOUTS, LIVE HACKS, TED TALKS AND EXPERT SPEAKERS.

FORUM HOST & AWARDS CO-PRESENTER
Alta Associates
FORUM HOST & AWARDS CO-PRESENTER
CSO

DIAMOND SPONSORS
accenture
High performance. Delivered.

CISCO

ini
Carnegie Mellon University Information Assurance Institute

Microsoft
U.S. BASKETBALL GREAT Michael Jordan once said, “Talent wins games, but teamwork and intelligence win championships.”

Cybersecurity professionals may not want to win national titles, but they also don’t want to lose to their opponents—the cyber criminals constantly conjuring up new ways to invade their networks and steal digital assets. And just as Jordan says, the most successful CISOs and security managers hire smartly and create superstar security teams that stand out for both their work and the way they work together.

With the worldwide shortage of information security professionals, finding the right talent at the right price isn’t easy. But it is possible. It starts with having a vision, a roadmap and recruiting know-how.
FIRST UP: A GOOD PLAN
Before the hiring can begin, cybersecurity managers must develop a roadmap with a shared vision that all team members understand and abide by, according to Deidre Diamond, founder and CEO of Cyber Security Network (CyberSN), a cybersecurity staffing company based in Boston.

“Today, security practitioners are so looking for that,” she says. “They’ve had quite a few years of a lack of a plan, a lack of a vision—you must have a vision and a plan to execute against for your security, or…you can’t build a great team.”

That vision has to start with team management, according to Michael Buckwell, CISSP, manager of information security at Windstream Communications in Akron, Ohio. “Clear direction and support from the top is key [and] sets the tone for what’s expected.”

He warns that there is a price to pay if that direction is lacking. “The keys to success for a team are to have a strong sense of purpose and make sure that the activities align with the mission. Otherwise, you’re just spinning wheels.”

FIND THE TALENT (BEFORE THE TALENT FINDS SOMEONE ELSE)
The shortage of cybersecurity practitioners creates a challenge in the hunt for information security talent. The latest (ISC)² Global Information Security Workforce Survey released in 2015 projected a shortfall in the global information security workforce of 1.5 million by 2020. There simply aren’t enough qualified professionals to keep up with what is already a $170 billion industry this year, according to Indian-based market research firm MarketsandMarkets. Supply simply can’t keep up with demand.

Yes, technical knowledge is a must, but cybersecurity leaders say they look for something in addition to computer science or engineering experience.

Dom Glavach, CISSP, is the CISO at Concurrent Technologies Corporation (CTC) in Pittsburgh. He looks for someone who “really has the piece that I call passion: passion about cybersecurity and a genuine curiosity.” That passion is key, he adds, because work in the cybersecurity field is not 9-to-5. “There’s not a clock or a time card you can punch. It’s continuous learning, continuous curiosity and always on the move.”

Buckwell underscores the need for dedicated cybersecurity practitioners. “One of the first things I look for is the desire and hard-work effort for the team more than about technology…actively staying current, connecting to the industry, anything the individual can do to show they are committed.”

Finding those passionate, dedicated cyber stars takes work, cautions Diamond. “Put yourself out there. Talk to people out there. Have something to sell—you’re in a sales position when you’re hiring. We’re talking about the cream of the crop that’s out there. They’re getting tons of phone calls. They’re getting tons of messages on LinkedIn. If one wants to grab these folks, one must be impressive.”

DESIGNING THE TEAM
But does a group of passionate, dedicated individuals make a great team? Not necessarily, according to a research project by Google.
During a two-year period, Google’s human resources department conducted more than 200 interviews with members of the 180-plus active work teams at the multinational tech company. Google released its results in the fall of 2015, posting them on its re:Work blog, The Water Cooler (https://rework.withgoogle.com/blog/five-keys-to-a-successful-google-team/). The main takeaway, reported Google research analyst Julia Rozovsky: “Who is on a team matters less than how the team members interact, structure their work and view their contributions.”

That interaction among team members is key, agrees Windstream’s Buckwell. “I do look to see how they are going to mesh with the team and the organization as a whole. I particularly look for people who can build bridges, have a humble attitude—that they are a tech expert but know there’s a wide range of knowledge needed.”

Personalities need to be complementary, says CTC’s Glavach. “It’s very, very important, because you are working so closely with people throughout the course of a day, a month, a year. So having a diverse mix of personalities is important, but having groups of individuals that fundamentally see and perceive things the same way [is crucial].”

Don’t underestimate the need for training, warns CyberSN’s Diamond. “This is a [relatively] new industry. There’s nobody who knows everything. And those that really do know almost everything are too few, so we must be willing to educate, and we must be willing to train. And the teams that are sticking together, the teams that have wonderful cultures, they have vision, and they have constant education.”

SOMETHING’S NOT CLICKING
Just because a team has the best and the brightest, the team itself may not “stick together.” Where to begin to find the problem? Ask the team, advises Diamond.

“A lot of times, managers are fixated on what they think is the answer to ‘what’s not working,’ and there’s another answer they’re not seeing. If a manager can’t answer their own ‘what’s not working,’ then they’re probably in their own way.”

That communication between the team and the manager is critical. “I think when things aren’t clicking, it’s usually a matter of communication,” says CISO Glavach. “One of the struggles working with good cyber people is that we tend to spend a lot of time in front of the keyboard, maybe dim the lights in the office, and focus on the terminal in front of us. And we tend to lose focus on good communication.”

Problems may go deeper than communication breakdowns, counsels Glavach. “If that wasn’t the issue, maybe we would look to ensure the people who are doing or are operating that particular cyber area have the appropriate skills and have the appropriate mentorship.”

Take a hard look at the environment, he adds, because the status quo may be a concern. “With small teams, sometimes people are overburdened or overtasked, and it’s just normal. It becomes so normal that you don’t pay attention [to the reality] that people are failing because they’re drowning.”

At some point, though, warns Buckwell, it might be time for tough decisions. “[It’s] worth a conversation, [but know] that the time spent with one individual is at the expense of the team as a whole. At some point, you have to take action.”

MOVING ON ALL CYLINDERS
Maintaining cohesion and forward momentum will continue as long as managers are paying attention to the work and the people.

CTC’s Glavach knows the pressures. “If you consider what cyber people do, they watch attacks, monitor for attacks, see anomalies. You’re constantly either on the
defensive, or you’re responding to someone else’s success, and that pace tends to take its toll.”

Look for ways to buoy up the team, he says. “When we have that bit of failure feeling, we take a Friday afternoon and do something innovative, do something out of the box that exercises our craft. It’s a morale booster.”

Windstream’s Buckwell adds that the team leader needs to keep the team motivated, including having “a clear understanding of how the team and the individual contribute to the overall organization. If the manager understands the value of what the organization is producing and is accepted and respected by upper management, that can be very motivating. The manager needs to bring his or her A game.”

**THERE IS NO ‘I’ IN TEAM**
In order for the team to succeed, there must be trust among its members.

“Trust is the lubrication that makes it possible for organizations to work,” advised the late Warren Bennis, a renowned leadership authority, scholar, author and adviser to business executives and presidents.

Professor Amy Edmondson of Harvard University calls a successful team dynamic “psychological safety.” Individuals share ideas and take risks without fear.

Whether it’s a Michael Jordan looking to teammates to pass him the basketball in the last seconds of the game or a cybersecurity professional relying on team members to keep the company safe, it’s a group effort by individuals coming together to create a “championship” team.

DEBORAH JOHNSON is managing editor of InfoSecurity Professional.
Talking Cybersecurity with Two Cool Cats

JIM DAVIS and his cartoon creation, GARFIELD, have been entertaining millions of fans since 1978 through comic strips, books, television shows and, soon, a new movie and a musical for children’s theater. They both recently talked with InfoSecurity Professional about their new partnership with the Center for Cyber Safety and Education.

The world’s most popular (and cynical) cat hopes to parlay his worldwide, multigenerational popularity to promote Safe and Secure Online, the program that goes into classrooms and senior centers around the world to teach users of all ages important internet safety tips.

What drew you and your team to partner with the Center for Cyber Safety and Education?

JIM DAVIS: (ISC)² has the biggest and best membership representing the interests of cybersecurity on the face of the earth. Garfield likes the biggest and the best. Also, Garfield is an international character, and this is a global organization.

We’re also interested in anything related to the internet because there are fewer newspapers these days, and everything once paper is going digital.
Any new territory is always open to the ill intentions of a lot of people seeking to take advantage of people's lack of education and knowledge of the new medium. That's why we need to make sure that our fans, our readers, have a safe and enjoyable experience.

How much did you know about cybersecurity before you accepted this gig?

GARFIELD: I thought that it was a video game. Now I know that it isn’t a game at all.

And what have you learned since to prepare for your new role?

GARFIELD: “Never believe anything you read on the internet” —Abraham Lincoln. I read that last week on Facebook.

Why is Garfield ideal to be a cybersecurity spokescat?

JIM DAVIS: Garfield is big and bright and speaks in very simple terms. He has the ability, by virtue of being a cartoon, of making a convoluted subject easy to understand. He can say things that perhaps others couldn’t because he’s Garfield. After 38 years, he has some credibility. He also has a cool factor with youth because he doesn’t follow the rules.

Any personal experiences you care to share to drive home the need to better educate children, teachers and parents on the roles each plays in cybersecurity?

GARFIELD: Well, for one, I was really disappointed to learn that you can’t eat the cookies online.

Have you had any personal experiences with cybersecurity issues?

JIM DAVIS: Every day. We have two full-time IT professionals who watch our networks all the time and who thwart the daily attempts to get through our firewall from all over the world. I recall one time I was giving an interview, when all of the sudden, our system came under attack. I watched as our website started spewing out these .jpegs. We had a complete shutdown, but we lost some of our art before we could respond.

Cats seem to get a lot of attention on the internet, especially on YouTube. Why do you think that is? And how do you plan to leverage such feline notoriety to get your message[s] across?

GARFIELD: It is true: cats rule, dogs drool. But, enough about Odie. I’ll get my message across using my usual charm, intelligence and publicity machine.

Would you consider yourself as much an activist as you are an artist?

JIM DAVIS: Part of being an artist is bringing a lot of possible solutions to a single problem. The definition of creativity is having several approaches to a single subject. We see lots of ways to address education and to help people develop a curiosity about different things.

Tell us about Dr. Cybrina, CISSP, since she’s new to your fans.

GARFIELD: She’s OK in my book. It’s cool to be cyber-savvy!

What do you see Garfield doing to help with cybersecurity education?

JIM DAVIS: He is at your service to help make more people aware of whatever the most pressing issues of the day are, as determined by the (ISC)² organization and membership. We can “Garfieldize” information to make it entertaining so it helps with the recall rate. We don’t pretend to know cybersecurity, but we do pretend to know Garfield.

Your celebrity spans generations—children and their parents and grandparents know you. Do you feel a lot of pressure to achieve critical acclaim in this new role?

GARFIELD: I don’t do the whole pressure thing. I leave that up to Davis.

What do you hope will be the impact once the Center introduces Garfield through Safe and Secure Online?

JIM DAVIS: I think he’ll have a tremendous impact because he has a lot of credibility with young people all over the world. He runs in 38 languages, and we’re now in our third generation of Garfield readers. We have a pretty broad reach.

The Safe and Secure Online program is geared primarily toward schoolchildren, but last year it branched out to seniors. If it’s not too impolite, how old are you in cat years, and can you relate to the senior experience, especially when it comes to being aware of online dangers?

GARFIELD: Well, let’s just say, in dog years, I’d be dead. I can relate to the senior experience. Wait—what was the question?
ON THE AGENDA at a recent security conference was a session titled “Why Johnny Can’t Write Secure Code.” The presenter designed the title to be tongue-in-cheek, but it underscores a constant, growing issue: the lack of security embedded into the software development process. This is particularly problematic for those who design web applications that are ripe for exploitation.

Last year’s Imperva Web Application Attack Report showed a threefold increase in SQL injection attacks and a 2.5 times increase in cross-site scripting attacks. The most recent Open for Web Application Security Project (OWASP) list of the 10 most critical web application security vulnerabilities also highlights how easy exploitation remains and shows the dire state of application security.
There are, however, opportunities for improvement. They start with a more information security-centric understanding of what it means when teams and organizations adopt agile software development practices. And to do that, information security professionals should also work to better understand today’s application development processes.

UNDERSTANDING AN INCREASINGLY AGILE WORLD

“Agile” software development refers to a style rather than a singular defined methodology. The “Manifesto for Agile Software Development” summarizes agile development’s basic tenets, and the “12 Principles Behind the Manifesto” expands upon those core principles.

Based on that manifesto, an agile style of development will include:

- A lightweight empirical process;
- Extensive and regular customer collaboration;
- Self-organizing and self-managing teams;
- Rapid feedback;
- Interpersonal communication;
- Just-in-time work;
- Limited documentation; and
- Measuring success based on working software.

There is no “one true agile”; multiple development processes can and have truthfully claimed that they are agile.

GETTING INTO SCRUM WORK

According to Version One’s 10th Annual State of Agile Survey, Scrum is currently the predominant form of agile that companies have adopted (58 percent), with another 10 percent using a Scrum/XP (Extreme Programming) hybrid.

Scrum is a “process framework for complex product development.” It focuses solely on project management and says nothing about how the developers have actually written the software. That’s one reason developers frequently augment it with XP development practices.

In a Scrum/XP project, work to be done is described as a “user story,” a short sentence describing the desired functionality in business terms. It contains a role, a goal and a reason. An example could be, “As a bank customer, I want to withdraw funds from my checking account so I can increase my cash on hand.” In a Scrum/XP project, user stories replace all the traditional forms of requirements, such as system functional specifications, business requirements documents (BRDs) or detailed requirements documents (DRDs). Some teams identify user stories before they kick off a project, but they will identify additional stories continuously throughout the project and add these to the backlog. Since a user story describes a piece of functionality, the team can develop and deliver it independently of other stories.

Sometimes described as “a reminder to have a conversation,” user stories are placeholders for later collaboration. Teams collect user stories in a “product backlog” and sort them by order of priority. A business user of the system, or their proxy, acts as a “product owner” and is responsible for which user stories are in this backlog and for ordering them based upon their business value. The product backlog contains “everything that the team might work on.” All the development work the team will undertake takes the form of a user story in the backlog or as part of a user story. There is no separate project plan or requirements document, aside from the product backlog.

READY TO SPRINT

To deliver software early and continuously, scrum teams work in “sprints,” or short iterations. Most teams today are using one- to two-week sprints. In that time, the team agrees to a scope of work for the sprint (based on which user stories from the backlog they agree to deliver). Then team members design, write code, test and deliver the user stories as working software during the same sprint.

Because the user stories are light on specifics, the team needs to have continuous access to the product owner to discuss possible ways to achieve the business goal and to verify that the completed function works to the business’ satisfaction.

“Agile approaches leverage ‘last responsible moment’ decision-making, allowing the latest, complete information and data to guide us,” says Lowell Lindstrom, past managing director of the Scrum Alliance and founder of the Oobeaya Group, an agile transformation services firm.

“As teams learn to use agile approaches, the skill and discipline of how to defer a decision, and when not to, are critical.”

At the start of the sprint, the team holds a sprint planning ceremony and creates a sprint backlog. This sprint backlog contains the user stories from the product backlog the team is committing to deliver at the end of the sprint. As part of sprint planning, the team will discuss with the product owner what the user story entails, and many groups will choose to document these as acceptance criteria. Once the necessary parties commit to the scope of a sprint, the scope does not change.

During the sprint, the team holds a daily stand-up meeting, or “scrum,” at which time each person answers three questions: “What did you do yesterday?” “What are you going to do today?” and “Do you have any blockers?” The last question refers to where the team needs help and what kind.
The daily scrum lasts no more than 15 minutes, and it’s the primary coordination meeting for the team. It allows everyone to know who’s working on what and what obstacles the team is encountering. A person in a formal Scrum role (the “scrum master”) takes ownership of resolving any blockers and is responsible for making sure the team follows the scrum process—including protecting the team from outside interference during the sprint. The scrum master, product owner and team are the only roles in a scrum project.

At the end of the sprint, the team holds a sprint review, also known as a “showcase” or “sprint demo meeting,” for project stakeholders. The purpose is to show the user stories they have completed, to preview upcoming work, and to gather feedback from the stakeholders. As the representative of the business on the team, the product owner is typically responsible for this ceremony, although that person may call on the team to assist.

More mature agile organizations are moving toward scaling agile practices beyond the team. Many of these approaches, such as the Scaled Agile Framework (SAFe®), incorporate Scrum/XP practices at their core. Understanding how to incorporate security requirements into a Scrum/XP project is therefore foundational for today’s security professional.

INCORPORATING SECURITY REQUIREMENTS INTO A SCRUM PROJECT

User stories describe the entirety of work the team will undertake, so user stories must incorporate security requirements.

In a traditional style of development, a security requirement might take the form of a stand-alone functional
requirement, such as “all access to individually identifiable patient data must be logged.” Using Scrum/XP, the user story describing where such data is accessed will need to include that sort of functionality.

Because the product owner is responsible for user stories—including their priority in the backlog and what it means to be “done” with them—the person filling this role must have an appreciation of the security requirements.

Some teams find value in documenting nonfunctional requirements, such as logging and performance, in a common location for easier reference and updating. These should not be thought of as stand-alone requirements but rather as a reference the team should review as part of the discussion of any user story and its acceptance criteria. Sometimes a given requirement will apply to the story in question. Sometimes the requirement may be slightly different from standard performance requirements. And sometimes it’s not in there at all.

When considering how to incorporate security requirements into user stories, it’s useful to think of a two-level scheme for security requirements. At the upper level are “capabilities” the system under development should have, such as role-based access control, nonrepudiation or confidentiality of data at rest.

When discussing a user story, the product owner and team also should consider what a given capability means in the context of this story. For instance, they should ask, “Does this story require nonrepudiation?” Any such requirements then become part of the acceptance criteria for that story, and the team will need to verify them before they consider the story complete.

“The development team can automate and test for many of these broader, nonfunctional requirements through a continuous integration process, allowing the security team...
to scale across projects,” says Ed Bellis, CTO at Kenna Security and former CISO at Orbitz.

“There are hooks into CI servers to use tools such as Gauntlet that allow the development team to perform security testing of these requirements during integration,” he continues. “A security team will need to rely on both tools and appointed developers within the scrum in order to scale.”

Kathy Marshak, agile transformation coach and SAFe program consultant trainer at Icon Technology Consulting, offers some tips for integrating security-related requirements into a Scrum or SAFe project.

“Ensure that security experts understand agile fundamentals so they can participate in discussions about definitions of ‘done’ and contribute to reusable acceptance criteria,” she says. “Ensure that coding standards integrate security practices [and that] such standards facilitate XP’s ‘collective code ownership’ practice. Encourage developers who are skilled in writing secure code to pair with other developers to spread the secure coding practices.”

Because they are business experts, some product owners are not technical and may not understand what security capabilities a system should possess and in which stories they should appear. While a scrum team has a single product owner, it makes no statements about who can provide input to the product owner. In fact, the development team frequently calls upon product owners to take input from multiple stakeholders, and security is another voice providing input.

The product owner and team can call upon security professionals to provide additional information as necessary; however, this requires the product owner to appreciate security’s importance in the development process. It’s our job as security practitioners to make that case.

By incorporating security capabilities into the user stories in a Scrum/XP project, we dovetail with the way modern application development works. This avoids disruption to the process and incorporates security requirements early and throughout the development process.
It's Showtime!

Garfield cues up to teach cyber safety lessons to his youngest fans. **BY PAT CRAVEN**

Well, this is it. After a year in the making, we are poised to unveil the first in a series of new cyber and internet safety lessons for younger children starring the world’s favorite cat, Garfield!

On our newest website, www.SafeAndSecureOnline.org/children, you will see the first of many features to come. It has been so much fun working with the great people at PAWS, Inc. to create this groundbreaking program based upon safety tips provided by you—the members of (ISC)².

Online, you will find a new interactive cartoon, along with a flipbook/comic book, and some great safety tips. You will also see the Educator’s Kit that is available for purchase. The kit will contain everything you or a teacher needs to teach a cyber safety lesson to 30 children. It will have a slightly different video than what you see online and include group discussion guides and safety-skills-related activity books, stickers, posters, trading cards and more.

Plans are to produce 12 different lessons during the next several years (it takes three to four months to do all the creative work for a single kit and cartoon) to address many of the most pressing topics facing children around internet safety. All the materials for the first lesson are available in English, but we have already begun working on translated versions to be released in 2017 and beyond.

All this work is not going to change the world unless we get it into the hands of the children who need it most, and this is where we need your help in two tangible ways.

1) **Help spread the word.** Tell people about the new materials on the website, but also talk to your local teachers, educators and school leadership about adopting the program for all their students. Many schools require internet safety training annually and are looking for something fresh that will keep the students’ attention. Garfield can do that for them.

2) **Volunteer.** Put on a presentation for children in your community—whether it’s at a local school, library, community center, place of worship, Scout meeting or anywhere children gather.

While it is no longer required to be an authorized volunteer to use the materials, we still encourage you to do just that. To become an authorized volunteer, you will need to submit an application, pass a criminal background check and complete an orientation/training (Note: Despite what you hear from Garfield, there is no requirement to like lasagna to become an authorized volunteer). Only those who successfully complete all of these steps will be permitted to represent the Center during presentations and other functions.

If you don’t complete the process above, you will be representing yourself or your company and not the Center during your presentations. We are also in the process of developing a digital badge for those who are authorized volunteers. If you are already a volunteer under the old program, you will be automatically moved to the new system. To learn more about becoming a volunteer, contact Annie Woods at awoods@isc2.org.

So now it is Showtime! You have the tools and resources...let’s go make it the cyber world safer. Then we can eat!
MARY N. CHANEY

Pennsylvania resident Mary N. Chaney is originally from Cincinnati and has been an (ISC)² member for eight years. A lawyer and former FBI special agent, she currently is senior director of corporate information security for Comcast.

EDITED BY ANNE SAITA

What made you want to pursue a career in information security?

Information security was a natural fit for me. As an information systems major with a law degree and as a former federal cyber-crime investigator, I took to the field like a fish to water. I continue to remain excited and thrilled about the industry and look forward to offering my services on how to shape it going forward.

Which was more difficult, passing the bar or passing the CISSP exam?

Sorry, (ISC)², but the Texas Bar was 2.5 days; one full day of multiple choice, one full day of written essay, and a half day of all Texas law, essay and multiple choice. No comparison—the bar exam was harder!

In what way(s) does your legal career help with your cybersecurity one?

My legal career has helped me tremendously in my career in cybersecurity. Being able to articulate how the information security controls put in place help protect (or not) the legal culpability of a company in the aftermath of an incident has proven to be one of the more powerful tools in my arsenal. Sitting in the room and being able to translate between lawyers, technologists, regulators and law enforcement is a wonderful skill to have.

What was it like being a special agent for the FBI?

Being a special agent for the FBI and investigating cyber crime was a great experience. Not only did I investigate cyber, but I was able to do some pretty cool things outside of cyber. But I can’t tell you what they were!

Being a federal investigator and determining exactly how a crime is committed is the ultimate root cause analysis. Thinking like a criminal is important in cybersecurity because ultimately, there is a human behind every crime. If you can understand their motivation, you have a good shot at knowing how to protect yourself.

Based on your previous jobs, what do you expect to do at Comcast?

In my new role, I will be a part of a small team that has the responsibility for blending strategy and risk to work on design strategy, risk management and assessing the effectiveness of operations for their three core business units, Comcast, NBCUniversal, and Comcast Spectator.

What do you believe is the biggest cybersecurity issue for children and their parents today?

The biggest issue for parents is not monitoring the content/access kids have to technology from the time they give them a device. My poor kids are 11 and 9 and have iPads of their own, but they can’t get to anything on those devices without my consent. Plus, they have to listen to mommy lecture them about creating secure passwords, geotagging, knowing who you are talking to online, never giving out our home address, etc.

Kids are kids; they are curious and believe that they are smarter and more savvy. A healthy bit of fear about the dangers of technology will always help!

If you had to start all over again, is there anything you’d do differently?

Absolutely not. I have had the pleasure of doing some great things while following my dreams, and I would not change a thing.

An expanded version of this interview will appear in the October issue of Insights, a companion e-newsletter for the (ISC)² membership.
Why blow your budget on piecemeal, ad hoc content generation?

Use our full-service creative agency dedicated to delivering your unique message.

Unleashing strong ideas and creating effective content marketing that is on brand and on time is our specialty. Twirling Tiger Media, a creative agency with its roots in journalism, is a team of expert storytellers and designers who will connect your customers’ business issues to your company’s solutions through original and honest content—the type that will attract, acquire and engage your target audience.

Drive profitable audience action with our services, which will be on brand with your company’s marketing goals.

Articles  Infographics  Publications
Blogs  Inspirational Quotes  Social and Digital Media
Case Studies  Leadership Guides  Sponsored Content
Content Marketing  Magazines  Success Stories
Custom Content  Newsletters  Web Content
eBooks  Press Releases  White Papers and more!

For how our team of experts can serve you, please contact Bob Ostrow at bostrow@twirlingtigermedia.com.

Twirling Tiger Media is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC) and federally designated as a Women-Owned Small Business (WOSB).
(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 EMEA
18-19 October 2016
Dublin, Ireland • Croke Park Stadium
emeacongress.isc2.org • #ISC2congressEMEA

SECURITY CONGRESS LATAM
29-30 November 2016
São Paulo, Brazil
isc2latamcongress.com • #ISC2congressLATAM

SAVE the DATE!
25-27 September 2017 • Austin, Texas • JW Marriott Austin
congress.isc2.org • #ISC2congress

© Copyright 2016. (ISC)², Inc. All rights reserved.
Have confidence in your cloud security knowledge.

Become a CCSP and lead your organization to the cloud.

Be a leader in the field.

CCSPs report that in addition to employer confidence, they have gained respect, credibility, and trust across all levels within their organization. CCSP certification on your resume will demonstrate your cloud security expertise and show employers that you can fill a void in the rapidly growing aspect of information technology that is cloud security.

CCSP tops “The Next Big Thing” list as the #1 certification survey respondents plan to earn in 2016

Download the CCSP Exam Outline