MAKE ROOM FOR MILLENNIALS
They are changing the way we work

GDPR
PRIVACY BY DESIGN AND BY DEFAULT

CHANGE
FROM RESISTANCE TO ACCEPTANCE

SOFTWARE
LET’S FINALLY DEMAND BETTER
The 5th Annual (ISC)² CyberSecureGov takes place

MAY 9-11, 2017

at the Marriott Wardman Park in Washington, D.C.

Join us as we bring experts from inside and outside of the beltway for this 3-day training event, addressing the human element of cybersecurity through the workplace. This educational platform will shift the focus of improving security from grooming the cyber elite to strengthening the broader community through effective cybersecurity education. This year you will have the opportunity in Educating the Workforce in Cyber.

Some of the topics for this year’s event will include:

- Cloud Security
- Threats Intelligence
- Critical Infrastructure Protection
- DEVOPS
- NIST CSF - Identify, Protect, Detect, Respond, Recover
- PROF - Professional Development
- BUS/FIN/RISK - Business, Financial, and Risk Implications
- IDM - Identity Access Management
- PRIV - The Privacy Challenge
- DEMO - Game-Changing Solutions

Now is the time to register for CyberSecureGov!

(ISC)² members can earn up to 20 CPEs.
features

PEOPLE-CENTRIC SECURITY

14  Make Room for the Millennials
Among the key findings in the new (ISC)² Global Information Security Workforce Study is the growing influence of younger cybersecurity professionals that is forcing employers to think differently about recruitment and retention. BY ANNE SAITA

GOVERNANCE, REGULATION AND COMPLIANCE

18  Privacy by Design and by Default
If you haven’t already, it’s time to consider how to bake privacy and security into your products and services before it’s too late. The second in a series on GDPR. BY HARVEY NUSZ

CHANGE MANAGEMENT

21  Transforming Resistance into Acceptance
Not everyone reacts to change the same way, and it’s important if you are a change agent or the one being forced to do things differently to both understand and work with people resistant to change. BY PAUL SOUTH

departments

4  EDITOR’S NOTE
Why We All Need Help
BY ANNE SAITA

6  EXECUTIVE LETTER
Let’s Learn to STEAM Ahead
BY DAVID SHEARER

8  FIELD NOTES
Discounts on FAIR training; the newest President’s Award winner; and more.

10  NEXT CHAPTER
Austin Chapter spotlighted.

12  MEMBERS’ CORNER
It’s Time We All Demanded Better Software
BY RAJ GOEL

25  CENTER POINTS
What Went Into the 2017 Global Information Security Workforce Study
BY PAT CRAVEN

26  5 MINUTES WITH...
Fatma Bazargan
Career advice from the United Arab Emirates’ first woman CISSP.

4  AD INDEX

Cover image: JOHN KUCZALA. Image (above): ENRICO VARRASSO.
editor’s note

BY ANNE SAITA

Know When to Ask for Help

EARLY IN MY JOURNALISM CAREER I worked at a newspaper where the editorial editor had a certain air about him. He was polished and polite and the other reporters respected his articulate prose (if not his politics).

So it was a huge shock when we learned a few years later this same man had been found frozen to death inside a heatless shack. All of us could not reconcile the debonair man we once knew with the desolate one in the news.

Yes, this is an extreme example of the consequences from failing to ask for assistance (and mental illness certainly played a role here). But on a milder scale, how many times have we fallen down a rabbit hole of resentment, pain or panic because pride or fear blocked us from asking, let alone accepting, help?

We all get overwhelmed at times. Some of us are workhorses who don’t want to turn down new projects or assignments, though we should. Others of us are so in need of approval that we unconditionally accept whatever is asked of us, even when we shouldn’t. Then there are those unprepared for a particular task and too embarrassed to admit it.

If work isn’t distributed—and accepted—evenly within a team, we grow resentful, make ourselves sick and burn out. That’s no way to work, let alone live.

So what can you do? First, acknowledge when you need help before your work and your health start to suffer. It may mean temporarily reassigning some tasks until you catch up. Or it may mean bringing in professional help to better manage a more permanent situation. It may even mean moving to a position better suited to your skills.

Striking the right workload balance doesn’t mean giving in, it means getting things done. If you need some assistance, ask for it or find a healthy way to ease an unsustainable situation. Otherwise, you risk being left out in the cold.

Anne Saita, editor-in-chief, lives and works in Southern California. She can be reached at asaita@isc2.org.

—Anne Saita, editor-in-chief

advertiser index

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

ISC²® CyberSecureGov .................................................. 2
ISC²® Security Congress .............................................. 5
ISC²® CCSP .............................................................. 7
ISC²® EMEA ............................................................ 29

Twirling Tiger Media .................................................. 27
Center for Cyber Safety and Education ......................... 28

©Rob Andrew Photography

©Twirling Tiger Media

Twirling Tiger Media is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC). This partnership reflects (ISC)²’s commitment to supplier diversity.

www.twirlingtigermedia.com
(ISC)² Security Congress conferences make a global impact 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 LATAM
07-08 JUNE
São Paulo, Brasil • Amcham Convention Center
isc2latamcongress.com • #ISC2congressLATAM

SECURITY CONGRESS APAC
03-04 JULY
Kowloon, Hong Kong • Sheraton Hong Kong & Towers
apaccongress.isc2.org • #ISC2congressAPAC

SECURITY CONGRESS
25-27 SEPTEMBER
Austin, Texas • JW Marriott Austin
congress.isc2.org • #ISC2congress
executive letter

BY DAVID SHEARER, CISSP

It's Time For Us to Gather STEAM

IT’S AN EXCITING TIME at (ISC)² as we unveil the results of our biennial Global Information Security Workforce Survey. It drew a record response of almost 20,000 cybersecurity professionals, providing a snapshot of where we’ve come as an industry—and what remains to be done.

We intend to release several micro reports from the survey throughout the year, particularly a couple focused on where we stand in attracting and retaining women and other underrepresented groups to help fill a well-documented shortage of cybersecurity professionals. It bears repeating that it is in everyone’s best interest to create a more diverse workforce if we are to continually combat threats and protect our organizations.

We need to draw from all levels of talent, and from a broad range of applicants representing different genders, races, ethnicities, educations and experiences. That outreach also needs to include those with liberal arts backgrounds. Most of us are familiar with the acronym STEM, which stands for science, technology, engineering and mathematics. In recent years, however, the arts have been introduced as an important part of problem-solving complicated issues, so much so that educators now prefer the term STEAM to recognize the creative community’s contributions to our increasingly tech-centric world.

Consider what happens if you continually use the same pen testers to find vulnerabilities. They tend to look at your networks and systems through the same lens. By diversifying, through crowdsourcing, and varying pen testers responsible for your evaluations, you tend to uncover new issues because these newcomers approach things differently.

A more diverse cybersecurity workforce expands problem-solving possibilities. The bad actors, after all, are extremely creative in their exploits. So it makes sense to engage people with liberal arts backgrounds to provide a different, inventive approach to combating cybercrime.

By having a broader range of experiences gathered for a common goal, organizations stand a better chance of creating solutions to prevent increasingly sophisticated attacks. This also requires mutual respect for the skills that each person brings to the group and being receptive to the ideas introduced by those who think differently.

In turn, hiring officials need to create welcoming environments for new team members. This is highlighted by some survey results, which show how different generations view their jobs and the role their employers play within it. Such a shift will likely require some accountability and housecleaning within a company’s current leadership.

I’m encouraged by some initiatives and minority-focused cybersecurity organizations that are raising awareness for a more diverse workforce—and way of working. For instance, scientific studies have shown that women, in general, are more effective at blending both the left and right parts of the brain. So as we move toward a more STEAM-oriented offense and defense, let’s consider how women are uniquely qualified to unite creative and analytical approaches to help us all form more robust solutions.

That sounds to me like a win-win.

David Shearer, CISSP, is CEO of (ISC)². He can be reached at dshearer@isc2.org.
RESPECT.
CREDIBILITY.
TRUST.
CONFIDENCE.

Prove your expertise with the #1 cloud security certification by (ISC)² and CSA. CCSP will propel you to the next level of your IT security career.

www.isc2.org/ccsp
James McQuiggan, CISSP, Gets ‘Upstaged’ with (ISC)² Award

As a first-time emcee for last year’s annual Information Security Leadership Awards (ISLA) in Orlando, James McQuiggan was a little nervous onstage at the lively awards program. That anxiety only grew when (ISC)² CEO David Shearer stood at the podium and told McQuiggan—and the audience—he was going off script.

The reason soon became obvious: McQuiggan himself was receiving the (ISC)² President’s Award, which recognizes volunteers who have made significant contributions to the organization through their volunteer efforts.

“It takes a lot to surprise me, and this time I was completely surprised. I was speechless,” said the CISSP from Orlando, where he’s a product and solution security officer for Siemens. In his 20s, he worked in the theater industry as a stage manager. After eight years, he decided it was time for a career change and began his path to a cybersecurity career.

He said he learned the value of volunteering from his mother, who often took him along when she volunteered for Meals on Wheels. Among his volunteer efforts, McQuiggan is a member of the North America Advisory Council, the incoming president for the Central Florida Chapter of (ISC)² and a huge advocate of the Safe and Secure Online program.

The schools-focused program, he said, is the contribution he holds dearest. “Being able to help develop and implement presentations for children, parents and seniors is extremely rewarding.” He’s been presenting Safe and Secure Online to fifth-graders for several years, since his two daughters, now 17 and 14, were in elementary school. His wife, a schoolteacher, and children were on hand to see him receive the President’s Award. And, as a bonus, he got to meet Garfield creator Jim Davis.

“There have been few nights in my life that I did not want the evening to end, and this was one of them,” McQuiggan said.

NEW MEMBER DISCOUNTS FOR FAIR TRAINING

(ISC)² members now have discounted access to RiskLens’ analytics platform built on FAIR. Members will receive 50 percent off of FAIR training, which is the international standard model for risk quantification. They will also receive a 30 percent discount on an annual subscription to RiskLens.

When it comes to cyber risk, information security professionals and their boards often speak a “different language,” making it difficult to understand the impact of decisions and demonstrate ROI. The RiskLens platforms help a CIO or CISO articulate cyber risk into business terms.

To learn more, visit http://www.risklens.com/isc2_risklens_partnership.
RECOMMENDED READING
Suggested by Larry Marks, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL

**Bitcoin and Blockchain Security**
By Ghassan Karame and Elli Androulaki
(Artech House Publishers, September 1, 2016)

**INCE BITCOIN TECHNOLOGY** first appeared in 2009, it’s been researched for use-cases in various firms across industries. *Bitcoin and Blockchain Security* by Ghassan Karame and Elli Androulaki is a crisp, engaging book outlining the architecture for payment systems and describing the protocol specifications for a generic blockchain system. Before your enterprise decides to implement bitcoin technology, a review of this book could enhance efforts to protect against the attackers that are ever present.

Bitcoin transactions are a chain of digital signatures. It allows the expenditure of coins that can be publicly tracked. It is an innovative technology that causes vendors to accept fast bitcoin payments to transactions without confirmations; that is, without requiring that these transactions are confirmed in blocks. Zero confirmation transactions are insecure.

The authors describe the various threat vectors for attacking bitcoin as well as several methods to thwart attacks. The authors warn that the security of transactions in the blockchain cannot be guaranteed as long as less than 50 percent of the network miners are honest. The authors do a masterful job of presenting the overall network architecture and exposing the risks of implementing and using blockchain.

The book mentions how an adversary that controls more than 50 percent of the computing power in the system can, in theory, double-spend transactions, prevent transactions from being confirmed, prevent honest miners from mining valid blocks and so on. This is one of the reasons that the authors stress the need for, and give examples of, designing security into the architecture.

There’s lot of math in the book used by the authors to describe the cryptography design and the private keys, but not very much information describing the types of wallets on the market today. Perhaps that is for a second volume.

This is a valuable reference to maintain in your library, primarily if you are a security professional, developer, or someone who is engineering-minded and wants to learn how bitcoin works. The strength of this book is that the authors have identified security threats, countermeasures and controls that may be researched and implemented to mitigate the potential of bitcoin and blockchain security risks. The reader can collect these to use for future reference or to review the planned design of such technology.

The author did not receive financial compensation from this publisher, nor a free copy of this book. All opinions are his alone.

---

THE MIRAI BOTNET

**Disrupted 900,000 Deutsch Telecom (Germany) users**
**Infected 2,400 TalkTalk Routers (U.K.)**

Source: Wired magazine, December 2016

Ninety percent of all data in the world has been created in the past two years. The challenge is that 90 percent of data is now unstructured. CIOs must build the data and analytics framework to help analyze that data and present the insight to allow the business to grow.

—STEVE PRENTICE, Gartner vice president and Fellow
STARTING WITH FEWER than two dozen members, the Austin (ISC)² Chapter has grown into a scholarship-raising powerhouse in just three years. With a current membership of more than 150, the chapter raised the most money in the recent Scholarship Challenge, a joint initiative between (ISC)² and the Center for Cyber Safety and Education. The members raised $3,409. The first $1,000 was donated (per challenge agreement) to the Center for Cyber Safety and Education and the remainder will fund two $1,200 scholarships for high school students in the Austin metro area.

Founded and incorporated as a nonprofit charity in 2013, the chapter started as a dues-paying organization ($40 per year). An early sponsorship from Cisco and current sponsorship support from Indeed.com and BitDefender.com has helped the chapter grow. As a result, member dues have been waived for the last three years.

President Tony Howlett, CISSP, credits the Scholarship Challenge with providing the chapter with the impetus to spread the message of the importance and the needs of the information security sector to educators and students. “This scholarship was the first time we did it by talking to school districts and counselors, just trying to make them aware of the opportunities out there and trying to encourage their kids to think about it.” He adds that the chapter is planning to extend that reach. “We intend to do more. We intend to do some focus on females in information security, encourage more girls to study it, be interested in it.”

The Scholarship Challenge was developed by (ISC)² and the Center for Cyber Safety and Education to generate awareness about the cybersecurity field and to encourage high school students to pursue related studies in college. (ISC)² chapters raise funds to offer their own scholarships to local high school students who are planning to pursue studies in cybersecurity. 

---

(ISC)² AUSTIN CHAPTER SPOTLIGHT

(ISC)² Austin Chapter Wins Inaugural Chapter Scholarship Challenge

From left to right: Pat Craven (Center Director); Bart Lauwers, CISSP, (Membership Chair); Louisa Hoberman, CISSP, (VP of Operations); Wes Simpson ((ISC)² COO); Tony Howlett, CISSP, (President); Dennis Sutherland, CISSP, (Treasurer); Bill Thompson (Meeting Committee).

“This scholarship was the first time we did it by talking to school districts and counselors, just trying to make them aware of the opportunities out there and trying to encourage their kids to think about it.”
—TONY HOWLETT, CISSP, (ISC)² Austin Chapter president
Q&A ▶ TONY HOWLETT, CISSP

In Search of the ‘Best and Brightest’

Chapter president discusses successful outreach efforts.

Congratulations on leading the pack in scholarship fundraising! What impact do you hope the Austin Chapter’s efforts, both financially and in outreach, will have in bringing more students into the cybersecurity field?

By encouraging young people to consider information security and assurance as careers, and making the education for those fields a little bit less daunting, we hope to attract the best and brightest to both private and public employment. The daily deluge of news articles about hacked companies and government entities means we need to have the best defending our country, its institutions and its corporations.

With the shortfall in staffing for tech sector jobs, especially in the cybersecurity field, what suggestions do you have for both educators and information security professionals to encourage and recruit more people to the field?

The promotion of the high salary ranges and interesting work that infosec professionals do is part of this. There can also be a patriotic part of this, with our military needing information security-savvy recruits to bolster our cyber-defense and -offense forces. One example of this [locally] is a cyberpatriot program for high schoolers that sponsors contests for creative cyber techniques. Several of our scholarship applicants went through this program. And it applies to all countries, not just the U.S.

With the stiff competition for donations to a wide variety of nonprofits, what fundraising advice would you give to other (ISC)² chapters to help them succeed?

We were able to offer the naming rights to a scholarship for the highest donor, which attracted several high bidders. We were able to offer the naming rights to a scholarship for the highest donor, which attracted several high bidders.

SCHOLARSHIPS OFFERED BY (ISC)² CHAPTERS FOCUS ON ADDING TO THE CYBERSECURITY TALENT POOL

With the pressing shortfall of information security professionals, (ISC)² chapters are stepping up efforts to attract and engage college students to the field. Scholarships are now available from many chapters, including Tampa Bay, Fla.; Richmond, Va.; and Austin, Texas.

The Tampa Bay Chapter is offering two scholarships to local high school students planning to pursue degrees in cyber, information, software or infrastructure security.

Two $1,000 scholarships are available to students currently enrolled in high school and residing in the Tampa Bay area. Eligible students must be planning to enroll in a college or university within two years.

Also offering two scholarships for local high school students planning to pursue degrees in cyber, information, software or infrastructure security is the (ISC)² Richmond Metro Chapter.

Ivan Gil, treasurer of the Richmond Metro Chapter, said there are two scholarships of $250 each available to students currently enrolled in high school and residing in the Richmond-Metro area.

For more information on (ISC)² scholarships, visit https://iamcybersafe.org/scholarships/chapter-scholarship-challenge/.
A Bitter Pill

Stronger software liability would fix much of what ails us.

“Software is eating the world.” –Marc Andreessen

“If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.” –Gerald Weinberg

Both of those quotes give us much to ponder. Software is eating the world…and shoddy software is caving in on us. Consider:

- **Medical device** (pacemakers, insulin pumps, medication dispensing robots, etc.) hacks as assassination tools have jumped from spy thrillers and TV shows to real-life possibilities, as demonstrated by University of South Alabama students and reported in *Computerworld* in September 2015.

- Almost every major brand of **car** (Jeep, Mercedes, BMW, Tesla, Ford, etc.) has been hacked in tests, according to a July 2015 *Wired* report.

- **Web browser** security is an oxymoron. Seeing every major browser get hacked at pwn2own has become a rite of passage, as well as big prize money as posted by Trend Micro in March 2016.

- **Adobe Flash** is the poster child for massively insecure software. Steve Jobs famously banned it from Apple products, describing his concerns in 2010 in an online post.

I’ve long advocated for us to adopt software liability laws. And a typical response is: “We’ll never get rid of zero-days.”

I believe that, as an industry, we fetishize zero-days a bit too much. Yes, they exist and are used in some attacks, but the vast majority of attacks succeed due to insufficient patching, inadequate monitoring and shoddily developed software.

But, since people like to bring up zero-days, let’s put that to bed.

The most impressive zero-day attack that occurred in the real world, in my opinion, was the 1982 Chicago Tylenol murders. An unknown individual (or individuals) bought Tylenol bottles in the Chicago area, opened them, added cyanide capsules to the bottles and replaced them on the store shelves. Seven people died as a result. No one was ever caught.

With millions of dollars at stake, not to mention public safety, Johnson & Johnson took what was at that time an extraordinary approach—a massive product recall. “Before 1982, nobody ever recalled anything,” said Albert Tortorella, a managing director at Burson-Marsteller Inc., the New York public relations firm that advised Johnson & Johnson. Its board and management decided to put patient safety first. Breaking with industry tradition, they went
public with the details. They offered a free recall of every Tylenol bottle in America. The recall cost Johnson & Johnson more than $100 million, and it initially lost market share.

In less than a decade, not only did the company regain market share, it exceeded its previous market share for over-the-counter pain relief medication. As a footnote, Johnson & Johnson and the pharmaceutical industry developed tamper-proof packaging, caplets, and made secure, tamper-proof packaging an industry requirement.

Another excuse for opposing software liability regulations: “I can’t do anything about it—it’s too big an issue.” Here is a case study that refutes that claim.

Fed up with shoddy and dangerous food production practices (rotting meat, vermin, animal feces, excessive workplace injuries, etc.), Upton Sinclair wrote the expose *The Jungle* in 1906, leading to massive public outcry and the eventual passage of the Pure Food and Drug Act, the precursor of the U.S. Food and Drug Administration (FDA), which arguably has saved more lives than any other act of Congress.

The Pure Food and Drug Act also led to thousands of food manufacturers and patent medicine manufacturers going bankrupt. Big or small, if they couldn’t produce food safe for human consumption or so-called “elixirs” that weren’t poisonous, they weren’t allowed to sell their wares.

A third common excuse for not supporting software liability laws: “Software is too complicated and too important to the economy to be regulated.”

Every industry, like every company, begins as a startup. That includes railroads, manufacturing, telecom, automobiles and software. As industries mature, they become central to the economy. Billions of dollars are made by a handful of individuals or firms that focus on generating profits and externalize safety costs.

It usually takes horrific accidents or a large number of deaths to capture the public’s imagination and/or require these industries to change practices. I strongly recommend you watch *Modern Marvels: Engineering Disaster,* a History Channel docudrama, to see how industry after industry (grain processing, sugar processing, bridge construction, stadium construction, shipping, etc.) investigated failures, developed new standards, made them mandatory and improved society.

The industry closest to software, in my mind, is the cigarette industry.

In the 1920s, cigarette manufacturers advertised their cigarettes as weight-loss products and adding sex appeal. By the 1950s, as revealed in later litigation, the cigarette industry knew that smoking tobacco caused cancers and other health issues but the dangers were not commonly known. It wasn’t until the 1990s when 40 U.S. states joined a class-action lawsuit that led to $206 billion in fines, elimination of cigarette marketing to children and a robust anti-smoking education campaign.

As information security professionals, IT managers or simply end users, we are the crash test dummies for software developers and until we start telling the truth to ourselves, our clients and vendors, we will keep suffering from compromises due to faulty products.

The Mirai botnet, a collection of 400,000 infected bots ready to create DDoS attacks, is not an accident. Nor is Business Email Compromise (BEC) an unintentional industry. Ransomware did not arise by chance, either. All are the result of decades of commercial incentives that let developers ship software with no security, no controls and no responsibility.

I think it’s time we drew lessons from history and started agitating for software liability reform. It’s 2017 and we’re overdue for an overhaul. We need to apply existing consumer protection laws to software, revoke EULAs and uphold our right to buy only software that’s fit for safe use.

In my mind, only two industries exist in the United States with zero consumer protection laws: illegal drugs and software. And both industries call their customers “users.”
SALARIES ARE UP in information security, especially if you work in healthcare or the military. Going forward, though, companies will need to do much more than provide good pay to lure the talent they’ll need to keep up with cyber threats and replace retiring baby boomers.

Among the key findings in the just-released Global Information Security Workforce Study (www.iamcybersafe.org/research) is the way the front lines of cybersecurity are being reshaped by newcomers to the industry—recent college graduates specializing in information security-related fields and older men and women ready to launch second or third careers.

Their welcomed entry comes at a time when companies, nonprofits and government agencies are finding it increasingly difficult to protect a proliferation of digital assets now commonly stored in a diffused IT architecture thanks to the rapid adoption of mobile platforms, cloud-based technologies and the Internet of Things.

The 2017 Global Information Security Workforce Study shows a younger generation is becoming a major force in information security, and employers must change recruiting strategies to find and keep them.

BY ANNE SAITA

The 2017 Global Information Security Workforce Study is a joint project supported by (ISC)², the Center for Cyber Safety and Education, Frost & Sullivan and Booz Allen Hamilton. Input in survey development and outreach was provided by the Executive Women’s Forum and the International Consortium of Minority Cybersecurity Professionals. Read more about the study’s methodology and findings at www.iamcybersafe.org/research.

PHOTOGRAPH BY JOHN KUCZALA
“We all know that the cyber landscape is increasingly challenging as the sophistication of bad actors and the severity of incidents grow,” said Angela Messer, a Booz Allen Hamilton executive vice president and leader of the firm’s cyber business. The company has been a major supporter of the global workforce study since its inception.

“Our industry must be innovative not only in its tradecraft, but also in how it supports employees through opportunities for skills development to meet today’s threats and prepare for tomorrow. At Booz Allen, we provide for this by offering traditional training and covering certification or advanced-degree program fees, as well as nontraditional learning opportunities, such as our Kaizen capture the flag platform and hacker space labs.”

During the last global study two years ago, analysts determined there would be a worldwide shortage of 1.5 million professionals needed by 2020. A wide gap still exists, though it may start to narrow as millennials, those born between 1982 and 2000, become the largest demographic in the global workforce.

This year’s survey drew a record 19,641 respondents, thanks in part to greater outreach and a shorter survey time. The last survey, which took twice as long to complete, drew 13,960 respondents. Almost 11,000 who took the survey are from North America (Canada and the United States) and more than 7,000 are not (ISC)² members.

Results from the survey will be released over 2017 in micro-reports (see this issue’s Center Points column for more details). Among the trends that were emerging as this article was being put together, about a month after the survey closed, was the growing impact of global millennials.

**GEN Y RESHAPING THE WORKFORCE**

There are the challenges from battling an increasingly sophisticated cyber army of criminals. And then there are the challenges of hiring well and holding on to that talent in order to stay ahead of threats.

Millennials, sometimes also known as Gen Y, are expected to represent 75 percent of the global workforce by 2025, according to a PriceWaterhouseCoopers report released a few years ago. In the United States, millennials are expected to comprise half of all workers within the next three years, according to the same report.

To add some perspective, consider that not only will your company’s workforce reflect this shift, so will your user base.

This generation is the most ethnically diverse and most highly educated. They believe in lifelong learning and, having grown up with the internet and social media, have a better understanding of global markets and movements than previous generations at their age. Personal and professional development and work/life balance tend to trump pay as their primary job incentives. Career advancement is also a major factor in whether they stick with an employer—even

---

**Who Took the Survey?**

19,641 respondents

<table>
<thead>
<tr>
<th>Region</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa</td>
<td>557</td>
</tr>
<tr>
<td>Asia</td>
<td>2,821</td>
</tr>
<tr>
<td>Europe</td>
<td>3,694</td>
</tr>
<tr>
<td>Latin America</td>
<td>979</td>
</tr>
<tr>
<td>North America</td>
<td>10,584</td>
</tr>
<tr>
<td>Oceania</td>
<td>488</td>
</tr>
<tr>
<td>Middle East</td>
<td>518</td>
</tr>
</tbody>
</table>

---
**Impact of Millennials**

Results from the Global Information Security Workforce Study show how workforces are being reshaped by younger cybersecurity professionals.

** Millennials are the most diverse cohort of infosec workers **

<table>
<thead>
<tr>
<th></th>
<th>Percent of infosec workers who identify as Caucasian</th>
<th>Percent of infosec workers who speak more than one language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boomers</td>
<td>78%</td>
<td>37%</td>
</tr>
<tr>
<td>Gen X</td>
<td>69%</td>
<td>59%</td>
</tr>
<tr>
<td>Millennials</td>
<td>65%</td>
<td>66%</td>
</tr>
</tbody>
</table>

** Percent who say role diversity is very important **

<table>
<thead>
<tr>
<th></th>
<th>Percent who believe organizational training programs are very important</th>
<th>Percent who believe executive leadership programs are very important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boomers</td>
<td>58%</td>
<td>24%</td>
</tr>
<tr>
<td>Gen X</td>
<td>60%</td>
<td>28%</td>
</tr>
<tr>
<td>Millennials</td>
<td>65%</td>
<td>36%</td>
</tr>
</tbody>
</table>

** Percent who have no security certifications **

<table>
<thead>
<tr>
<th></th>
<th>Percent who have no security certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boomers</td>
<td>6%</td>
</tr>
<tr>
<td>Gen X</td>
<td>9%</td>
</tr>
<tr>
<td>Millennials</td>
<td>21%</td>
</tr>
</tbody>
</table>

** Millennials value organizational training programs the most, but are most likely to be paying for their training themselves **

<table>
<thead>
<tr>
<th></th>
<th>Percent who are paying for their training completely themselves</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boomers</td>
<td>24%</td>
</tr>
<tr>
<td>Gen X</td>
<td>28%</td>
</tr>
<tr>
<td>Millennials</td>
<td>36%</td>
</tr>
</tbody>
</table>

** Millennials are the most likely to place value on mentorship and leadership programs **

<table>
<thead>
<tr>
<th></th>
<th>Percent who believe mentorship programs are very important</th>
<th>Percent who believe executive leadership programs are very important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boomers</td>
<td>58%</td>
<td>24%</td>
</tr>
<tr>
<td>Gen X</td>
<td>60%</td>
<td>28%</td>
</tr>
<tr>
<td>Millennials</td>
<td>65%</td>
<td>36%</td>
</tr>
</tbody>
</table>
more so than attractive compensation packages. They also look to their Gen X and baby boomer managers as mentors.

“The traditional hierarchy of a workplace is shifting,” notes Patrick Craven, director of the Center for Cyber Safety and Education, which produces the biennial workforce study. “While many Gen X survey-takers said they aspired to climb the ladder and become a CISO, their younger peers were more likely to see themselves as security consultants in the next two to three years.”

Within information security, the under-30 group is the least likely to hold a certification and most likely to want their employer to pay for their training and certification. “They believe in the power and strength of certifications, and most likely cite financial reasons for not having one yet,” Jason Reed, a Frost & Sullivan analyst, says.

When asked what they think their role will be in the next few years, millennials are most likely to say “security consultants.”

“They crave role diversity,” Reed explains. “So you can’t stick them in a silo and ask them to operate as a cog in the machine for a very specific thing. They need to have diversity in their workplace and in the roles that they fulfill. And that’s an adjustment employers need to make in order to ensure the ongoing success of their industry and their own organizations.”

Mirroring millennials in other industries, this generation of information security professionals tend to be mobile, insist on flexible work hours and speak more than one language. Leadership and mentorship opportunities are important to them, especially when their employer is willing to invest in their career advancement.

Another characteristic that sets them apart from their older peers: company loyalty, specifically the lack of it. The survey confirmed what employers already are experiencing: millennials are most likely to leave their employer voluntarily. (That may be partially because they are currently the least likely to be moored to a place by a home mortgage.)

This could create a quandary for employers concerned with turnover or expanding security teams to protect their assets and comply with data privacy laws and regulations, and who are seeking professionals who’ve proven competency by completing credential programs.

“In the near term, the way to retain talent requires employers to make adjustments to the way they relate to their young employees,” Reed says. “It requires them to offer financial support they need for training and leadership programs, including certification expenses.

“Another thing driving job satisfaction among young people is supporting remote or flexible work environments,” he adds. “That’s another thing people who recently left their jobs cited as a top driver of their job satisfaction.”

ANNE SAITA is editor-in-chief of InfoSecurity Professional magazine.

“**They need to have diversity in their workplace and in the roles that they fulfill. And that’s an adjustment employers need to make in order to ensure the ongoing success of their industry and their own organizations.**”

—JASON REED, analyst, Frost & Sullivan

---

40% of those who had the right number of security staffers said they could remediate a threat in one day, compared to 26% of those with “too few”

70% of hiring managers say that certifications are important when making hiring decisions

Percentages based on all survey responses

Highest Paying Industries

<table>
<thead>
<tr>
<th>Industry</th>
<th>Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>$109,000</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$108,000</td>
</tr>
<tr>
<td>Global Industry Average</td>
<td>$99,000</td>
</tr>
</tbody>
</table>

**“They need to have diversity in their workplace and in the roles that they fulfill. And that’s an adjustment employers need to make in order to ensure the ongoing success of their industry and their own organizations.”**

—JASON REED, analyst, Frost & Sullivan
Building Better Safeguards for Consumers by Baking Privacy and Security into Product Design

The EU General Data Protection Regulation (GDPR) will require stringent controls to protect individual privacy. As systems are developed or upgraded, “baking in” the required controls can prevent future violations. By Harvey Nusz, CISSP

At a 2016 Conference in New Orleans, after the EU General Data Protection Regulation passed, I asked a fellow attendee employed by an international retailer if the company had started its GDPR work. His company profiles customers to identify their potential purchases, and he responded with an immediate and emphatic “Yes!” His company was already studying how to implement privacy and security by design and by default—a key requirement of the GDPR that will take effect in May 2018.

What, though, about everyone else?
The concept of ensuring that personal data is protected during design was developed by Ann Cavoukian, Ph.D., the former information and privacy commissioner of Ontario, Canada. In 2009, she authored *Privacy by Design, The 7 Foundational Principles*, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. It is essentially privacy engineering, which NIST is working on now in a draft document, entitled “NISTIR 8062 (Draft) Privacy Risk Management for Federal Information Systems,” http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf. The purpose is to be able to understand the risks and to utilize controls that ensure that a subject’s privacy data are not misused or breached—not an easy goal to accomplish in today’s environment of frequent and high-profile data breaches.

**THE NEW RULES OF PRIVACY**

GDPR privacy protections are mandatory. These are spelled out in Article 25 – Data Protection by Design and by Default, as published in the Office Journal of the European Union:

“1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.”

(Note: The International Association of Privacy Professionals (iapp.org) defines pseudonymization as “the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately.”)

**WHAT ARTICLE 25 MEANS TO PRACTITIONERS**

My interpretation of this article is:

1. We should identify the key data protection principles, which include data minimization, and the controls that meet them, and implement them based upon the results of the Privacy Impact Assessment.

2. Essentially, we are being told to prevent a breach, whether we or our processor is involved.

3. We will monitor and demonstrate compliance, either internally or with external assistance.

**PUTTING THE RULES TO WORK**

There are several relevant principles, at a minimum, that should be implemented with appropriate controls and monitored for effectiveness in achieving proper security, privacy and compliance:

**Data minimization**

Know where your data is, particularly your sensitive privacy data, and purposely minimize it and its use. A privacy inventory is needed to achieve data minimization. Among other data elements contained, it should identify the systems in which data privacy elements are present and maintained.

**Purpose limitation**

Use proper design elements and review them to ensure that the original intent has not been expanded. If that intent is expanded beyond which you have received consent from the data subject, you could be subject to fines.

**Transparency in processing**

Tell the data subjects how you will collect, process, store and report their data, and conduct reviews to ensure that you, the controller and your processor(s) do just that.

The following three principles are not new, but I would argue that they have increased importance with the impending GDPR:

- **Confidentiality**: Keeping data subjects’ privacy data confidential to only those with a need to know.
- **Data integrity**: Ensuring that data subjects’ privacy data is not inappropriately modified.
- **Availability**: Ensuring that data and the systems that process it are available.
It will be a critical success factor in achieving GDPR to define and implement data categorizations for your privacy data.

THE IMPORTANCE OF CATEGORIES
It will be a critical success factor in achieving GDPR to define and implement data categorizations for your privacy data. In that categorization effort, it will be important to understand and identify the privacy data you collect for workforce members, customers, vendors, partners and any others. The next step is to categorize that privacy data according to its sensitivity, describe it in your policies, procedures and processes, and provide training. Those categories will become very useful in your privacy impact assessments and your privacy (and security) by design and by default efforts, and in communication with your processor(s).

GOING FORWARD
As a part of your strategy for properly incorporating Privacy and Security by Design and by Default, your procedures should be baked into your PMO procedures to ensure consistency and repeatability. When designing procedures, utilizing the concepts presented in the NIST document, “NISTIR 8062 (Draft) Privacy Risk Management for Federal Information Systems,” will assist you in determining what is right for your organization. It is not too early to implement these measures and controls.

Achieving compliance by May 25, 2018 will require work now to ensure that not only new systems and systems with planned modifications properly and verifiably handle data subjects’ privacy data, but also that all systems are reviewed to ensure that all privacy data is handled appropriately. It will be important to document critical aspects of the decisions made, as required by GDPR, and to recognize and address any needed adjustments in those decisions when significant changes occur.

This also applies to all infrastructure projects, all processes whether electronic or manual and all business or institutional practices. Remember, the culture is changing, and as legendary management consultant Peter Drucker reminds us, culture eats strategy for breakfast. As we monitor for compliance to the GDPR, we may also want to monitor our culture.

In addition to creating a privacy inventory and privacy categories for your privacy data, also define your organization’s privacy lifecycle. By going through that process, and understanding and defining the lifecycle of the privacy data you collect and store, you will be better prepared to assess risk and protect the data.

MEETING THE REQUIREMENTS—STEP BY STEP
While there is much to do in a short amount of time, the following steps are recommended, at a minimum:

Develop a strategy that includes:
• Privacy impact assessments
• Assess your normal practices with respect to privacy data, and appropriately implement privacy and security (data protection) by design and by default
• Create, validate and maintain a privacy inventory
• Define your privacy lifecycle, and include expected and approved practices, and harmful practices to avoid in each phase
• Create and implement privacy categories
• Create and maintain data flows of privacy data
• Consider hiring or appointing a data protection officer early, and get that person involved in all your policies, procedures and processes around privacy data
• Continue to monitor, assess and improve.

Baking in the right controls the first time is far preferable to the alternative of bolting them on later, which usually results in significantly increased cost, and in missing the mark on managing risk.

By doing so, you’ll be set apart from your competition.

Deeper Dive
To learn more, visit http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

HARVEY NUSZ, CISSP, CIPM, CISA, CRISC, is a security and privacy consultant, and can be reached at PrivacyShieldGDPR@gmail.com.
IN NOVEMBER 1999, Ted Simendinger was atop the sales and marketing world. As one of the top salesmen for Xerox, Simendinger traveled throughout the company, training the copier giant’s sales force.

Changes were in the air at Xerox, as it moved away from the mechanical and toward technology. As he was en route to Honolulu, Simendinger was unaware that the coming changes had one employee—a veteran technology professional—feeling trapped.

“It was a big technology jump,” Simendinger says. “[The employee] was so worried about the change in technology that he snapped. He was seeing ghosts in every corner, [thinking] ‘They’re trying to get rid of me. I’ll never be able to do it. I’ll lose my job.’ The guy got in a negative vortex spiral, snapped and killed seven people.”

For years Simendinger mulled a one-word question when it came to the worst mass shooting in the history of Hawaii. “Why?” As he pondered, closing the sale became not as important as helping people navigate the sometimes treacherous waters of change. His life changed course forever.
“That gave me my mission, Simendinger says. “I knew when all that happened that my life had a higher purpose. It wasn’t to hawk copy machines any more, it was to help people get out of that pit of sadness and despair.”

He adds, “My life changed in a thousand ways.”

Now, Simendinger travels the world teaching organizations and individuals how to cope with change as part of developing successful life skills. He’s written books on behavior and change under the pseudonym Ocean Palmer. He’s lectured on six continents.

RECOGNIZING THE ROOTS OF RESISTANCE

While Simendinger’s epiphany borne of tragedy is an extreme case, getting employees to navigate and embrace change is a major challenge, according to (ISC)² member Tony Howlett, chief technology officer at Network Security Services, an IT consulting firm that works with banks, government and in healthcare.

“You are always going to encounter a little bit of resistance, but what it is and how much can determine the success or failure of an information security program.”

—TED SIMENDINGER, author

“It is a huge problem and can undermine all the technical controls put in place, as well as the good efforts by other employees, especially if this is at the executive level,” Howlett says. “If there are exceptions to policy made for management or execs, it not only basically says that the rules are not for everyone but also exposes accounts that are of higher value than the rank and file. It also sets up a legal issue if they want to take action against an employee for not following policy that is not enforced universally. You are always going to encounter a little bit of resistance, but what it is and how much can determine the success or failure of an information security program.”

In an earlier generation, when American industry was more bricks than clicks, resistance to organizational change often took hundreds, sometimes thousands, of workers on picket lines to silence scorching-hot steel mills or quiet cauldron-black coal mines.

Now, in the information age, it takes only one person to push back against a new idea or a new way of doing things. In the best case, that resistance slows change. But the resistance can cause actual damage: It can cost a small community bank thousands of dollars or big-box retailer millions in a security breach. And, in a worst-case tragedy, as in the Xerox shooting, fear of change can ignite workplace violence.

It begs a key question: How do security professionals and their teams successfully navigate the sometimes treacherous waters of change in order to calm potential fears and minimize resistance?

How to ‘Change’ It Up

In his blog, workplacepsychology.net, Dr. Steve Nguyen outlines leadership expert John P. Kotter’s 8-step process to creating major change:

1. Establish a Sense of Urgency: Examine market and competitive realities; identify and discuss crises, potential crises or major opportunities

2. Create the Guiding Coalition: Assemble a group with enough power to lead the change; get group to work together as a team

3. Develop a Vision and Strategy: Create a vision to help direct the change effort; develop strategies for achieving that vision

4. Communicate the Vision: Use every vehicle possible to communicate the new vision and strategies; have Guiding Coalition role model the behavior expected of employees

5. Empower Action: Get rid of obstacles to change; change systems or structures that undermine the vision; encourage risk-taking and nontraditional ideas, activities and actions

6. Generate Short-term Wins: Plan for visible performance improvements or “wins”; create those “wins”; recognize and reward employees who made “wins” possible

7. Consolidate Gains and Produce More Change: Use increased credibility to change systems, structures and policies that don’t fit the vision; hire, promote and develop employees who can implement the change vision; reinvigorate the process with new projects, themes and change agents

8. Anchor New Approaches in the Corporate Culture: Create better performance via customer and productivity-oriented behavior, more and better leadership, and more effective management; articulate the connections between the new behaviors and organizational success; develop the means to ensure leadership development and succession. •
FINDING THE ROUTE TO ACCEPTANCE

First, it’s important to understand the driving forces behind resistance. For some, faulty communication sparks push-back. Others resist out of panic or fear, while a few might respond out of hubris (“the smartest person in the room” syndrome).

The wheel of effectively navigating change involves four stops—awareness of the change, the panic stage, acceptance, and “flourishing in the new reality.” The challenge for leaders, Simendinger says, is moving an organization from panic to success.

“You’ve got to get them to accept it. Unless you get them to acceptance, you’re never going to get them to stage four, which is ‘flourishing in the new reality.’ The ship’s leaving. We’re shoving off. Are you on the boat or not?”

Communication is key, Simendinger cautions. And part of that communication is identifying key people of influence within the organization.

“The bigger the change, the more stuff has to be communicated. Gossip, the internet, social media and technology being what they are these days, if you don’t communicate the facts clearly, then the rumormongers and the gossips and the backstabbers and the politicians will fill in the gaps with nonsense. The bigger the change, the more important it is to communicate, communicate, communicate. I can’t stress it enough. The objective of the communication is to get them from the panic stage to the acceptance stage.”

TAILORING THE PLAN

There is no such thing as a cookie-cutter approach, warns Simendinger. “A good leader understands that people are herd animals, like sheep. Five sheep determine the direction of a flock in the field. If the five sheep decide to go over the hill, they start going and everybody else follows. Five sheep determine the direction of the flock. The behavioral dynamics of an organization are the same way. There will be peers of influence in the workplace who can be your five sheep for you.”

Dr. Meng-Chow Kang agrees that there is no “one-size-fits-all” approach, especially in the context of the global economy. Kang, a director of security and trust for Cisco Systems in Singapore and a board member of (ISC)², sees how cultural and policy differences also come into play when addressing the dynamics of change.

“Indeed, this is critical in global organization. The way we go about it is to make sure we are consistent in our policy principles and practices. It doesn’t mean one size for all or set a lowest common denominator so it can be followed by all. Rather, it is to allow for apples-to-apples comparison.

Six Steps to Manage Resistance to Change

According to leadership consultant Dr. Steve Nguyen, there are six main reasons people resist change:

1. They don’t believe the change is necessary or will make things worse.
2. They don’t trust people handling the change effort.
3. They don’t like the way the change was introduced.
4. They are not confident the change will succeed.
5. They feel the change will mean personal loss—of security, money, status or friends.
6. They’ve experienced a lot of change and can’t handle any more disruption.

What can you do?

Encourage employees to openly express their thoughts and feelings about the change program.

Listen carefully to their concerns, explore their fears and take their comments seriously.

Engage them in the planning and implementation processes.

Identify those who have something to lose and anticipate how they might respond.

Help them find new roles either in your group or somewhere else in the organization—roles that represent genuine contributions and mitigate their losses.

“For example, in certain geographies, our business decides that the risk in country A is higher than in the U.S. Instead of setting up just a specific policy for country A, we look for a set of risk assessment criteria and policy requirements for different countries that we operate, and establish the risk ratings as a baseline for determining which country will need to step up more in terms of their security measures. In this way,” Kang sums up, “employees of country A know that they are not specially drawn out and being discriminated. Instead, they can find other countries in similar risk ratings that need to do the same.”

GETTING EVERYONE ON BOARD

Involving top management in the process is crucial, Kang adds. “Leaders in each country are also included to provide input in setting up the assessment criteria, and agreement
on the final risk rating assigned. Another important aspect is that security must be an enabler. As such, once they meet the policy requirements (in terms of implementing various additional controls, for example), they can now operate like any other businesses operating elsewhere. Without fulfilling those additional requirements, their access and actions will be constrained."

Training is also critical, Network Security Services’ Howlett stresses. And, change agents have to make the basis for change real.

"Four, five, 10 years ago, it was all theoretical. We didn't have breaches at all. Now companies are getting hit all the time. Ransomware is reaching down into retail. We have to make it real.

"If you give limited training and it's one-and-done, then it's almost worse than doing nothing. A few will remember for a while. But if you're not doing at least annual training or even more often, it's not going to make an imprint on the people. It's really important to follow up with training, testing. We now run automated phishing email tests all the time, so that if an employee is vulnerable to phishing, you find out sooner rather than later."

Along with education and training, Howlett recommends spot compliance checks. That may even include phishing email tests or “dumpster diving,” checking waste-paper baskets for sensitive material. "You'd be surprised at how often we find sensitive information in the trash cans of companies that have policies and procedures and shredders and shred cans readily available."

One individual, not the mass picket line of another generation, can cost a company millions, Howlett warns. “It doesn't matter what you do, or how many firewalls or high-end technologies you buy, it only takes one person not following policy to undo all that. You're only as strong as your weakest link. And it only takes one person who's trying a shortcut or doesn't understand.”

**THE FUTURE OF CHANGE**

Organizations are trying to tackle the “weakest link” using technology, such as behavior analytics (user, system and process analytics) and automation (e.g., automated cyber security detection and response), according to Cindy Cullen, president of the New Jersey Chapter of (ISC)².

“There is change under way that makes it less dependent on people. Most organizations are realizing that it’s very true—that it’s too people dependent. So they are making efforts to make it less people dependent.”

In the final analysis, Simendinger says, it comes down to individuals in key roles making a choice. “A manager inspects, delegates, tells you what to do. A leader, by my definition, inspires results through others. If you do that they’re going to embrace the change quicker. But if you're just a manager, they're going to challenge you because they want to know why…you get in all this taffy pulling that you don't need. That begs the question: What are your people—managers or leaders?”

**More Reasons for Resisting Change**

1. Fear of the unknown
2. Lack of good information
3. Fear of loss of security
4. No reason to change
5. Fear of loss of power
6. Lack of resources
7. Bad timing
8. Habits

Source: Schermerhorn, Hunt & Osborn, 2005

Here are some other resources to learn more about change management and human behavior.

*The Impact of Technology on Behavior and Happiness*, by Ocean Palmer; Airplane Reader Publishing, 2016

*Managing the Worry Circle*, by Ocean Palmer; Airplane Reader Publishing, 2009


*That’s Not How We Do It Here! A Story about How Organizations Rise and Fall - and Can Rise Again*, by John P. Kotter; Portfolio, 2016

*Implementing Change and Overcoming Resistance*, by Dr. Steve Nguyen, 2010
[https://workplacepsychology.net/2010/02/05/implementing-change-and-overcoming-resistance/](https://workplacepsychology.net/2010/02/05/implementing-change-and-overcoming-resistance/)

*6 Steps To Manage Resistance To Change*, by Dr. Steve Nguyen, 2010
[https://workplacepsychology.net/2010/05/13/6-steps-to-manage-resistance-to-change/](https://workplacepsychology.net/2010/05/13/6-steps-to-manage-resistance-to-change/)


PAUL SOUTH is a freelance writer based in Florida.
Fresh Data and New Insights from the Latest Global Information Security Workforce Study

IF YOU HAVE BEEN in the industry for a while, you've come to look forward to the release of the (ISC)² Global Information Security Workforce Study every two years. It is already here again and, boy, is it packed with some great new insights into the state of our workforce.

With 19,641 security professionals from around the world taking the time to answer some 100 questions, you can imagine the mountains of data we have to offer. In fact, it's too much data to provide to you in one sitting.

So this time we have scheduled a series of releases of “sub-reports” throughout the year. To make it even easier to digest, gone is the 48-page book of flat graphs and seemingly endless words that try to capture everything we learned. Our new reports will be shorter but full of even more information as we release them in multiple media formats, including printed executive summaries, infographics and interactive graphics on our new website www.iamcybersafe.org/research. We will release a report on millennials in the cybersecurity workforce on February 16, and the Women in Cybersecurity report on March 8. Our report on the cybersecurity workforce in the U.S. government will be published in May.

Because we live in a globally-interconnected world, we have expanded our analysis of the cybersecurity workforce.

For the first time, there will be reports about the workforce in the Europe/Middle East/ Africa (EMEA), Latin America (LATAM) and Asia-Pacific (APAC) regions as well as North America.

Also for the first time, we will publish a report on the diversity of the cybersecurity workforce in the U.S.

We are looking forward to presenting these reports to you in the coming months.

Between these formal reports, there will be updated information posted online as it becomes available. Make sure you go to our webpage www.iamcybersafe.org/research and sign up for update notifications. That way, you can stay informed when new information is released. You won’t be disappointed.

How did all this come about? First and foremost, you, the members, and your tremendous support of the project over the years have kept the enthusiasm high for investing the time and money it takes to complete a project of this magnitude. To say it is “years in the making” is an understatement. Trust me, we already are taking notes for the next study in 2019.

So “new and improved” doesn't do justice to this version of the Global Information Security Workforce Study. But I will let you be the judge of that.
Fatma Ahmad Bazargan, CISSP

Fatma Ahmad Bazargan was the first woman to earn a CISSP® in the United Arab Emirates. She is the head of information security at Injazat Data Systems and has been an (ISC)² member for 11 years.

I understand you are the first woman to receive a CISSP in the United Arab Emirates.
Yes, I’m the first Emirati woman to receive a CISSP, which I earned in 2006 and, to this day, that is the first comment I get when I meet other security professionals.

What made you pursue the CISSP certification?
CISSP, back then and today, is always seen as a renowned certification when it comes to information security and, because of that reason, I was keen to put in the effort to study and sit for the exam. Since then, I have maintained a good standing.

How difficult was it to study for the exam?
I attended the CISSP course here in UAE and then joined a two-day CISSP boot camp that was held in Las Vegas at the Interop conference in 2006. Once I returned home, I sat for the exam; being well prepared made it easier to pass.

What first led you to pursue information security as a career?
In 2002, I was a new graduate with a bachelor of science degree in computer engineering from the American University of Sharjah. I was offered, as an entry-level job, a position as a network administrator at Thuraya Satellite Company. While working there on various network components, I became fascinated with how firewalls and intrusion detection systems work. That was my turning point from IT to information security.

What did you learn from your very first job that helps you with your current one today?
My first job was the best starting point for me as it showed me how crucial information security is in safeguarding what is important to the organization and its “crown jewels.” Ever since 2002, I have watched the IT world grow and have learned much about its inner workings and about IT security operations and how it revolves around governance, risk, compliance and audits. It has been a great journey so far and I wouldn’t want to change a bit of it.

What keeps you up at night as a CISO?
I would say everything. As a chief information security officer we are focused every day on ensuring that the organization is safeguarded and secure, inside out. But the worry of the zero-day attack, the security of the contractors, the employees’ actions, the client’s network among the rest does occupy my mind constantly. After all, the irony is there is no 100 percent security and the attacker just needs one zero-day, or a single unpatched system, to get a foothold in your network.

You were pursuing a Ph.D.—what was your thesis focused on?
My Ph.D. thesis was focused around how to come up with an efficient and effective security monitoring solution in a cloud environment for mechanisms of early detection of cybersecurity incidents.

What was it like to receive a MESA award in 2016?
A privilege indeed. I have placed it on a shelf in my office and whenever my eyes fall on it I remember this entire career journey of what I have been through so far and I look forward to how it will continue to be more challenging, yet fun! *

An expanded version of this interview will appear in the April issue of Insights, a companion e-newsletter for the (ISC)² membership.
A NEW PERSPECTIVE ON YOUR BRAND’S NARRATIVE

Using words and images that are unique to your branding, Twirling Tiger Media can help you tell your company’s story cohesively across multiple content marketing solutions.

Contact Bob Ostrow, business development director, at bostrow@twirlingtigermedia.com
Scholarships

We are excited to announce that the 2017 (ISC)² Information Security Scholarship applications are now being accepted!

High School, Secondary School, Undergraduate and Graduate students from around the globe are encouraged to take advantage of this exciting opportunity and apply!

If you are currently, or will be, pursuing a degree with an information security or cybersecurity focus you may be eligible. Please help spread the word!

<table>
<thead>
<tr>
<th>2017 (ISC)² Scholarship Opportunities</th>
<th>Open to Apps.</th>
<th>Close to Apps.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women’s Information Security Scholarships</td>
<td>OPEN NOW</td>
<td>Mar. 9, 2017</td>
</tr>
<tr>
<td>Undergraduate Information Security Scholarships</td>
<td>Feb. 15, 2017</td>
<td>Apr. 20, 2017</td>
</tr>
<tr>
<td>Graduate Information Security Scholarships</td>
<td>Mar. 1, 2017</td>
<td>May 4, 2017</td>
</tr>
</tbody>
</table>

For complete eligibility requirements & application access

CLICK HERE

www.iamcybersafe.org/scholarships
Welcome to our first series of (ISC)² Secure Summits in Europe, Middle East and Africa!

(ISC)² Secure Summits bring multi-subject sessions from hands on practical workshops to keynotes and panel discussions featuring local and international industry experts to maximize the learning experience, networking and CPE opportunities.

(ISC)² Secure Summit BENELUX Amsterdam 4 - 5 April
(ISC)² Secure Summit NORDICS Stockholm 9 - 10 May
(ISC)² Secure Summit DACH Zürich 28 - 29 June
(ISC)² Secure Summit MENA Dubai 21 - 22 November
(ISC)² Secure Summit UK London 5 - 6 December

Learn more at: [edu.isc2.org/secsuresummits](edu.isc2.org/secsuresummits)

Free for (ISC)² members | Earn up to 16 CPEs.