HOW TO MAKE A CHANGE
IT CAN—AND MUST—BE DONE

GO DIGITAL OR DIE
CREATE POLICIES
PEOPLE ACTUALLY READ
GDPR YOU READY?
PLANNING FOR SECURITY CONFERENCES
ATTEND RSA CONFERENCE 2017 FOR LESS!

Save $200 with your (ISC)² member discount code.

From February 13–17, the (ISC)² community will come together in San Francisco at RSA Conference 2017, the world’s largest infosecurity event.

Join your peers and discover:

- Over 555 sessions covering a range of topics to help you stay on top of threats and solutions.
- (ISC)² CCSP Two-Day Crash Course covering the six domains in the Certified Cloud Security Professional CBK.
- (ISC)² CISSP Two-Day Crash Course covering the eight domains in the Certified Information Systems Security Professional CBK.
- More than 550 exhibitors in two Expo halls.
- Four days of enlightening and inspiring keynotes, led by speakers such as Dr. Neil DeGrasse Tyson, Dame Stella Rimington, Eric Schmidt and many more!

Visit www.rsaconference.com/isc2 to register today!
Use code 1U7ISC2FD when you register to save $200 off a Full Conference Pass.
features

PEOPLE-CENTRIC SECURITY

16 The Challenge of Change
Whether it’s a course correction or major organizational redirection, successfully navigating the potentially bumpy road of change takes planning, skill and support.
BY DEBORAH JOHNSON

CISO MANAGEMENT

20 Go Digital or Die
Businesses are adopting new virtual and cloud-based technologies at a rapid rate, sometimes too quickly. Learn what to do if your organization is on the fast track and security is getting left by the wayside.
BY ADAM WOJNICKI

SWISS ARMY KNIFE

25 Read Me
Streamlining your organization’s IT policies and procedures is long overdue.
BY KAREN CHAMBERLAIN

GOVERNANCE, RISK AND COMPLIANCE

28 GDPR
Now is the time to consider how the EU’s upcoming privacy regulations will impact your organization, regardless of where it is located. The first in a series.
BY HARVEY NUSZ
So often we start January committing ourselves to do better, which requires us to manage our time wisely to fulfill new goals. In our effort to gain more control over our schedules, we vow to prioritize better and accomplish more.

But all of our good intentions are easily sabotaged when we work with people who appear unwilling to do the same. That’s why people with a high EQ—emotional intelligence—recognize less productive colleagues and develop strategies to work better with (or in spite of) them.

They recognize that perfectionists value error-free work over deadlines, so they create interim due dates that embed more time for reviews. They manage expectations from both executives, who want strategic initiatives met, and operations centers consumed with continuous threat monitoring, security maintenance and incident response.

They also better manage themselves. They set priorities for the day, week, month and year and use project management tools to establish priorities and get things done. The most successful of us manage personal energy levels to maximize workloads—getting the most important items done first, when our energy (and perhaps caffeine) levels are at their peak.

They also know some days will go better than others, but when productivity dips turn from days to weeks with growing regularity, something has to change. Which brings us to our cover story on change management. There are different models for how to best bring about meaningful change within an organization, and there are numerous studies showing that we humans do not all accept change at the same rate.

But change is vital to any organization’s survival. That also goes for those who operate within it. Understanding more about change is the first step in creating it, within your organization and within yourself.

Anne Saita, editor-in-chief, lives and works in Southern California. She can be reached at asaita@isc2.org.
Interested in speaking at the 5th Annual (ISC)² CyberSecureGov? Call for Speakers is now open for submissions until midnight EST on FEBRUARY 1, 2017.

EDUCATING
The Workforce in Cyber

(ISC)² CyberSecureGov provides an educational platform to share lessons learned, best practices, and your expertise on today’s cybersecurity challenges. Hosted in the nation’s capital and attracting leaders in government, military, industry, and academia, CyberSecureGov will ensure that your voice is heard. This year you will have the opportunity to Educate the Workplace in Cyber within the framework of prevention, detection, and resilience. There are a limited number of sessions available, so submit your abstract now.

Session Topics include:

- Cloud Security
- Threats Intelligence
- Critical Infrastructure Protection
- Automation and Agility
- Identify, Protect, Detect, Respond, Recover
- Professional Development
- Business, Financial and Risk Implications
- Identity Access Management
- The Privacy Challenge
- Game Changing Solutions

#CyberSecureGov | May 9-11, 2017

Learn more about CyberSecureGov
Why We're Going it Alone at This Year’s Security Congress

FOR THE FIRST time in six years, (ISC)² will break away from a longstanding and successful partnership with ASIS International and host its own U.S.-based Security Congress. The conference will be held September 25-27 at the JW Marriott in Austin, Texas.

Year after year, attendees of Security Congress have shared that they want access to more information security exhibitors, to see a greater (ISC)² presence throughout the event and to enhance their learning opportunities.

The immense size of the ASIS event, with the large representation of physical security technology and product vendors, left only a small portion of the exhibit floor space allocated to cybersecurity. Our members felt the time was right to put the spotlight on cyber, and we agreed.

When asked why the 2015 Congress did not meet his expectations, one attendee replied, “I found that the co-location with ASIS only brought confusion. The exhibition was huge, but 99 percent of it was irrelevant.”

(ISC)² puts members’ voices first and is dedicated to making its members the best practitioners in the industry. As Congress has evolved, we have established brand values, such as transparency, value, and access to premier learning and networking opportunities. Making Congress an independent event is essential for us to deliver on those values.

The American Marketing Association defines a brand as the “name, term, design, symbol, or any other feature that identifies one seller’s good or service as distinct from those of other sellers.” Your brand identity is the representation of your company’s reputation through the conveyance of attributes, values, purpose, strengths and passion, and we want the Security Congress brand to be an industry leader when it comes to cybersecurity events and educational opportunities.

Feedback consistently indicated that (ISC)² members wanted their own event, with their own content catering to their specific fields. After careful planning, the decision was made to make the seventh annual Security Congress an independent event. Another key benefit of hosting our own event is the ability to hold additional preconference tracks across a variety of topics, as well as increase the number of key, thought-provoking speakers to engage with a broader audience.

(ISC)² is grateful to members of ASIS International for allowing us to co-locate with them during the past six years. Their support and guidance remains integral to the success of the Security Congress. We could not have gotten Congress off the ground without ASIS, but in the end, we need to put our members first.

Early-bird registration will open in spring 2017 at http://congress.isc2.org/.
CALL FOR SPEAKERS

Deadline: February 24

Sept. 25-27 • Austin, TX • JW Marriott Austin

Congress.isc2.org • #ISC2Congress
(ISC)² to Welcome New Chapters

BEGINNING IN 2017, (ISC)² will start accepting applications for new chapters, following a two-year hiatus. Chief executive officer David Shearer is enthusiastic about the addition of groups worldwide. “We are very much looking forward to welcoming new chapters early in 2017,” he said in a blog post. “We have taken the time to understand what is required to motivate success and are putting the finishing touches on solid foundations for the future.”

In 2015, (ISC)² stopped accepting applications for new chapters. The chapter program, launched in September 2011, had grown tremendously to 135 official chapters in more than 50 countries around the world. As interest continued to grow, (ISC)² leadership felt the time was appropriate to pause and review the chapter start-up process with an eye toward improving chapter operations and organizational support for the future.

Shearer sees the chapters as key to the future of (ISC)². “Chapters allow us to both support our membership on a local level, and pull topical experience from different parts of the world to gain a view on how these issues are affecting our members. The program informs how we move forward as a profession.”

FIVE NEW AND RETURNING MEMBERS JOIN (ISC)² BOARD OF DIRECTORS

Members voted and the following were elected to begin three-year terms on the (ISC)² Board of Directors:

- Arthur Friedman, CISSP, U.S.A.
- Sai Honig, CISSP, CCSP, New Zealand
- Jennifer Minella, CISSP, U.S.A.
- Greg Thompson, CISSP, Canada
- Zach Tudor, CISSP, U.S.A.

“We are very much looking forward to welcoming new chapters early in 2017.”

— DAVID SHEARER, chief executive officer, (ISC)²

Top 10 Skills Where IT Managers Report Shortages

1. IT security
2. IT architecture
3. Cloud computing
4. Network engineering
5. .NET development
6. Business analysis
7. Core skills
8. IT service management
9. Network operations
10. Systems engineering

Source: Global Knowledge, September 2016

Illustrations: Thinkstock

Where IT Managers Report Shortages

1. IT security
2. IT architecture
3. Cloud computing
4. Network engineering
5. .NET development

6. Business analysis
7. Core skills
8. IT service management
9. Network operations
10. Systems engineering

Source: Global Knowledge, September 2016

Illustrations: Thinkstock
POWERING THE NEXT GENERATION OF IT LEADERS

“Lack of sleep exacts an economic toll of more than half a trillion dollars per year in the United States, the United Kingdom, Canada, Germany and Japan alone.”


Simply saying that girls aren’t into technology or they’re not as good at technology as boys is a vast oversimplification and, frankly, not true.

—CAROLYN APRIL, senior director of industry analysis at CompTIA


Ready to advance your career in cyber security, information technology, and other high-demand fields? Walden University offers the degree programs you need to stay competitive—and become a leader in your field:

- Doctor of Information Technology (DIT)
- Doctor of Business Administration (DBA)
- MS in Information Technology
- Master of Information Systems Management (MISM)
- MS in Health Informatics
- Graduate Certificate in Information Systems
- BS in Computer Information Systems
- BS in Information Technology

GET STARTED NOW.
LEARN MORE ABOUT TUITION SAVINGS.
Meet the EMEA Region’s Saleema Adejumo

ALEEMA ADEJUMO IS one of four recipients recently awarded scholarships by the Center for Cyber Safety and Education in the EMEA region.

Currently a student studying for a master’s degree in security and risk management at the University of Leicester in the United Kingdom, Adejumo was selected for a Women’s Scholarship in 2016 after her first application was unsuccessful. “I decided to apply to the scholarship every year until I got it, and I did!”

Adejumo has worked as a system administrator since 2009. This is her first career and she plans to establish and consolidate her experience as a principal security consultant in the next 10 years. “I am an information/cybersecurity enthusiast and very passionate about research in the world of security, risk, vulnerabilities and cyber warfare,” she said. “I intend to fully transition from systems administration to information/cybersecurity in the next two years. The scholarship makes my medium and long-term career goals feasible; attaining my goals seems much more achievable.”

The Center for Cyber Safety and Education encourages diversity within the workforce and supports women entering the information security industry through its scholarship program.

“I have been fortunate to work and study in organizations that do not gender discriminate,” Adejumo said. “It is the reason I am so proud to be associated with the Center for Cyber Safety and Education. Placing an emphasis on scholarships for women will go a long way in increasing the number of women professionals in cybersecurity, thereby making the field even more open and accessible to other women. It is a very commendable venture and the Center deserves high praise.”

Congratulations, once again, to Adejumo and all of the 2016 scholarship winners. To learn more about 2017 scholarship programs, including key dates, visit the Center’s website at https://www.isc2cares.org/Scholarships for details and deadlines.

TIPS TO EFFECTIVE BOARD PRESENTATIONS

1. Tell the story through a strong simple narrative.
2. Make clear connections to business objectives.
3. Communicate in terms of risks, not threats.
4. Clearly and defensibly connect strategic goals to the risks.
5. End with an ask, identify next step.

Source: https://www.gartner.com/doc/3237924?srcId=1-6731482093&stl=0

By 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually, which is an increase from today’s 40%.

Time to Make Your Case

Video
DIGITAL ATTACKS—MALICIOUS HACKING—have become part of the daily news cycle and the constant worry of public and private institutions around the world. Chronicling the first major digital intrusion, cybersecurity journalist Kim Zetter, a reporter for Wired, dissects the success, story and color around the origin and impact of Stuxnet.

In *Countdown to Zero Day*, Zetter deftly describes the origin of Stuxnet: Why did it start? Where did the idea come from? What did its creators hope to accomplish? She charts, on a high level, the design of Stuxnet, what the modules were intended to do, how they protected each other, what their inputs were and how one of the modules remained resident without being detected. She tracks the best-intentioned efforts of Symantec to decipher and track down each of the objectives of the modules and other instances of Stuxnet, such as DuQu.

The international politics in play and their impact on homeland security are part of Zetter’s reporting. The zero-day exploits she describes cannot be completely prevented without significant security awareness and best efforts of a security operations center to detect, alert, prevent and minimize the impact of such exploits.

Zetter’s work may read like a gripping spy novel, but it tracks the real-life beginnings of today’s digital warfare in an engrossing way. ■

---

**TOP 10 Strategic Technology Trends for 2017**

1. Applied AI and advanced machine learning
2. Intelligent apps
3. Intelligent things
4. Virtual and augmented reality
5. Digital twins
6. Blockchains and distributed ledgers
7. Conversational systems
8. Mesh app and service architecture
9. Digital technology platforms
10. Adaptive security architecture

Source: Gartner, Inc.
FOUR YEARS SINCE its founding, the (ISC)² Kuwait Chapter is proving itself to be a significant resource to business, the community and, most recently, education. The chapter has secured a grant from the United States Embassy, Kuwait, Public Affairs Office to run a pilot program for Safe and Secure Online. With the help of the Center for Cyber Safety and Education and its new ambassador, Garfield, the program potentially will reach 40 bilingual schools in the country, helping 1,200 schoolchildren sharpen their skills on data privacy.

To drive Safe and Secure Online forward in Kuwait, the chapter this year appointed Dana Winner, CISSP, to the newly created board position of Education Chair. Winner will visit schools to help launch Safe and Secure Online, as well field interest from partners to help develop the program in Arabic.

“We are looking to create a movement, really change behaviors in the region,” Winner says.

Safe and Secure Online represents the latest achievement for the Kuwait Chapter, which was established in 2012 by Sarfaraz Kazi, CISSP, manager of the national security office at the National Bank of Kuwait (NBK). To find the 15 people he needed to apply to (ISC)² as an official chapter, Kazi researched the IT community and reached out to people he did not know to gauge interest.

“The response was very enthusiastic and it wasn’t long before the recruitment campaign moved beyond my co-workers at the bank to the wider financial services community and others,” he said. “I personally started to become known for my ability to network and bring people together, which has been very good for my development and even helped me earn a MENA Leadership Award last year.”

“We are looking to create a movement, really change behaviors in the region.”

—DANA WINNER, education chair, (ISC)² Kuwait Chapter

Tamer Gamali, CISSP, is the chief information security officer at NBK (and Kazi’s manager) and a key figure within the information security field in Kuwait. He was elected the chapter’s first president and assisted in garnering support from the local community. The Kuwait Chapter developed quickly, becoming the first in the Gulf Region to be chartered within the (ISC)² Chapter Program and working with the EMEA office to be an active asset in the development of (ISC)² in the region.

An increase in members evolved from the Kuwait Chapter’s participation in a one-day (ISC)² Secure Event conference with a program of speakers, including representation from the Kuwaiti government. “This proved to be a great way to cement our chapter’s reputation as an organization that could deliver strong educational content, allowing us to develop as a top forum for Kuwait’s information and cybersecurity community,” Gamali explained.

Today, the chapter, with a core membership of 60 professionals, stages quarterly education events that are open to the wider professional community, a fact that has helped establish the chapter’s reputation. “Everyone is able to come together and get to know each other in a spirit of mutual respect,” founder Kazi said.
A Side Conversation with Kuwait Chapter President Tamer Gamali

What do young people need to know most about being safe online?

The first is that they should be aware of the threats on the internet and what could happen. For example: receiving a suspicious email with an attachment could infect their computer, allowing a remote user to access all their data. Or understanding the consequences of posting personal information on social media, such as the fact that you are going on holiday on your unsecured profile, allowing anyone to know that your home is unoccupied.

In addition, when dealing with people, especially being introduced to people online, there are inherent risks since you don't actually know who that person is. There are many cases where people create a fake profile to entice the recipient to meet them and which could potentially result in harm to you.

People should be aware of the types of security software that should be installed on their PCs or mobile devices to protect them from typical online threats. In fact, user awareness is now regarded as the most important factor when being online; knowing what can go wrong and what to look out for can act as the best line of defense.

What are the young people’s (and many adults’) biggest misconceptions about being online?

Youngsters tend to post everything about themselves online to share with their friends. What they often don’t consider is that most information posted on social media is not private and could be misused. This may also impact their future prospects as many colleges and potential employers use search engines to find out information about them as part of the hiring process or background check. Users should be aware of this fact and conduct periodic research using a normal search engine to see what type of personal data is available for all to see. We are seeing more regulations regarding privacy with legislation such as “the right to be forgotten,” which allows an individual to request any potentially damaging information available online to be removed.

Another misconception is that people sometimes don’t consider the fact that online identities cannot be verified easily. There are cases where people are impersonating other people who you may know in order to obtain information about you.

A basic guideline is to always check your social media privacy settings and limit your social posts to friends, something many often don’t realize is possible.

How are you encouraging young users to investigate IT and/or cybersecurity as a major course of study leading to careers?

We host a lot of events in Kuwait and, on occasion, target the younger age group by inviting local schools and college students to attend.

We also share and demonstrate areas within cybersecurity, which may prompt the younger generation to ask questions about starting a career in cybersecurity or information security. Typically we respond by directing the interested people to education centers that offer career training.
5 TIPS
To Get the Most from Your Next Conference

MY FIRST LARGE technical conference was overwhelming. I didn’t know where to start. After several conferences, I can now share five tips for getting the most value from your conference experience.

1. **Know your goal(s).** Identify a primary goal and any secondary goals for attending the conference. For example: are you most interested in attending a class, getting CPEs or CLEs, networking, previewing products or working at the conference? Knowing your goals will help you plan your time.

2. **Plan ahead.** Identify any logistics or planning needed before you register. Consider registering for any limited-seat sessions, contacting vendors that you want to meet with and confirming a coverage schedule with your manager. Arriving at registration early, getting the layout and confirming hotel transportation will save you time battling the crowds. Review the final conference program to highlight sessions and exhibitors you want to see. Consider mapping your route through the exhibit hall to find your “must see” exhibitors. Take plenty of business cards to exchange.

3. **Prioritize your activities.** Take a few minutes each night to review your plan for the next day and select activities that support your goals. Take advantage of your conference’s mobile app to plan each day. Keynote speakers can be inspirational, while individual sessions can introduce you to a new topic or product. I have found networking lunches to be great for meeting people, but plan to arrive with enough time to engage others in conversation before any guest speakers are introduced. Decide when you will visit the exhibit floor and for how long. Find three to four sessions with topics that are new to you. If you are intrigued by a session, ask the speaker afterward if they are free for coffee or schedule a conversation later.

4. **Plan for the post-conference report.** Identify up to three topics of interest to you, your employer or related to your goals. Attend the sessions related to these topics. Think about how you will answer the question “How was the conference?” Take sufficient notes so you are ready to report on your time and show managers they made a good investment in sending you to the conference.

5. **Have fun.** We all work hard on a daily basis, and a conference is an opportunity to learn, get refreshed and to have some fun. If you are there alone, make some friends on the first day and plan to meet up with them later. Take part, responsibly, in the fun activities. You want to come back refreshed, with new ideas and renewed energy.

By knowing your goals, planning ahead, prioritizing activities, preparing a post-conference report and having fun, you will gain more value from your next conference.
(ISC)² delivers a series of one day conferences throughout North America as an added member benefit for (ISC)² members that includes the opportunity to earn CPEs. These educational events are designed to address the continuing education needs of infosecurity practitioners, focusing on those issues and challenges they are facing today and what may be looming on the horizon. Members tell us that the sessions are invaluable for connecting, learning and ensuring continued value within the roles that they deliver.

Secure My Spot

2017 Local Events

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan. 19</td>
<td>SECURE LAS VEGAS</td>
</tr>
<tr>
<td>Mar. 17</td>
<td>SECURE PHOENIX</td>
</tr>
<tr>
<td>Mar. 20</td>
<td>SECURE SEATTLE</td>
</tr>
<tr>
<td>May 9-11</td>
<td>CYBER SECURE GOV</td>
</tr>
<tr>
<td>Jun. 16</td>
<td>SECURE DENVER</td>
</tr>
<tr>
<td>Jul. 21</td>
<td>SECURE TORONTO</td>
</tr>
<tr>
<td>Sept. 25-27</td>
<td>SECURITY CONGRESS</td>
</tr>
<tr>
<td></td>
<td>(Austin, TX.)</td>
</tr>
<tr>
<td>Oct. 17</td>
<td>SECURE CHICAGO</td>
</tr>
<tr>
<td>Nov. 3</td>
<td>SECURE BOSTON</td>
</tr>
</tbody>
</table>
WITH APOLOGIES TO  American pop singer Jimmy Buffett, changes in your business latitudes require changes in attitudes from every level of the organization. Without that, corporate change can fail to take hold.

The numbers tell the disheartening story. In the 2013 Global Culture and Change Management Survey conducted for Strategy& by the Katzenbach Center of PwC, based in New York City, only 54 percent of the 2,219 corporate participants reported that their efforts at change succeeded—and lasted. The rate of failure can damage a company in many ways. More disappointing results were revealed in a 2012 study of 5,400 large IT projects by McKinsey, in collaboration with the University of Oxford (U.K.): 45 percent ran over budget and 7 percent were late, while delivering 56 percent less value than predicted. And, McKinsey reported, some failures cost so much in time and money that they endangered the future of the company.

So what’s an IT security professional to do to ensure success in managing change?
START AT THE TOP

Whether it’s a large organization with multiple departments involved, or a smaller business with a singular focus, there comes a time when a major change is mandated. Total support from the highest echelon is crucial. If it’s not there, major corporate change is doomed, as reported in 2014 by the Project Management Institute, based in Newtown Square, Pa. In its study of 723 project managers, Pulse of the Profession: The High Cost of Low Performance, 56 percent cited lack of leadership as the cause of failure and 59 percent cited insufficient communications.

The desire for change in a company can come from any level of the organization, according to Antonia Cusumano, principal and leader in the Global Human Capital practice at PwC.

“What matters is that the people who are driving the change, the people who are funding the change, make a commitment to walking the walk…ensuring there’s a budget…and helping the organization go through the change,” she says. “That’s where the rubber meets the road.”

Cementing buy-in from company leadership can require some different thinking on the part of the CIO, CSO or CISO, says Ron Ashkenas, partner emeritus at Stamford, Conn.-based Schaffer Consulting.

“The first step is to make the business case, not the technical case,” he advises. “They must say what are the financial implications, strategic implications, customer implications. What does it mean for the rest of our business? What are our competitors doing?

“You’ve got to make that case, just like any other investment. The CEO needs to look at IT as a strategic investment, not just a nice thing and ‘I’ll do whatever the IT guy tells me.’”

Seeking out executive supporters can enhance the chances for success. “Every change effort needs someone in senior management who’s a champion for [the change],” advises David La Piana, managing partner at La Piana Consulting in Emeryville, Calif. That way, he says, “the team that’s trying to lead the way can have somebody to talk to and who can push things out of the way that are stopping them.”

As team leader, your abilities are under scrutiny.

“Leadership must believe in you and in your abilities to execute the change,” according to Mack Bhatia, CISSP, fractional CISO and security director at Enterprise Integration, based in Jacksonville, Fla. Bhatia headed up the company’s move to SOC 2/SOC 3 compliance project (for which he won a 2016 (ISC)² Americas ISLA®).

He says you also have to ascertain that the rest of the company is on board. “You have to check these two key things first, because if the leadership doesn’t believe in you, that you are the right person to do the change, and if they don’t want the change, then it’s a moot point.”

WINNING ‘HEARTS AND MINDS’

In an organization, “change” can mean different things to people performing the various functions needed to keep the business going. The danger is in not communicating the details of the change deeply and widely enough.

Fifty-six percent of the managers queried in the 2014 PMI project manager study blamed “insufficient communications” for their project’s failure.

“The fatal flaw,” warns La Piana, “is that senior management, without actually consulting the people who have to carry it out, decided, in their wisdom, ‘This is what we have to do’ and then said ‘Make it happen.’ That is the death knell of most change efforts.”

He advises team leaders to get all the parties involved as early as possible. “Get senior management to actually include the people who need to make the change.”

PwC’s Cusumano agrees and underscores the need for clarity by leadership in “articulating the case for change—‘Why are we doing this?’ So that people can see the motivation, the purpose, the vision behind it…”

Aligning the various parts of the organization takes time and attention to how the employees involved in the project are reacting. Enterprise Integration’s Bhatia says you have to deal with any issues early on. “[There] was just a concern about how much work was this going to add to my daily tasks in some pockets of the organization. The idea was to
ensure that we coordinate this, we publicize the importance of this audit, so the chance that there would be resistance would be defused before it even occurs.”

Defusing potential interdepartmental friction is also crucial.

“Get the people who have to solve the problem in the room together with some leadership and articulation up front about what needs to get done and why…and give them a chance to work together to solve the problems,” advises Cusumano. “It doesn’t solve everything but, at a minimum, you break down barriers.”

La Piana agrees. “Get the different perspectives together at the very beginning.”

Cusumano also notes that cybersecurity has its own unique challenges when it comes to managing change. “With cybersecurity specifically, you’re asking people to think differently about how they, day after day, manage information, and the security of that information.”

She adds, “Looking at cybersecurity through the change management lens, it becomes really important to think through what [are] the critical few behaviors that need to change on a day-to-day basis to help you drive to a culture that now focuses on [new practices] as part of its everyday business.”

A CASE STUDY AT ENTERPRISE INTEGRATION

Implementing a major initiative has many parts, all of which must work in tandem. Enterprise Integration’s Bhatia, an (ISC)² member, had to deal with all those parts in overseeing a major institutional change for his company.

Understanding the vision

Bhatia was tasked with significantly reducing the outsourcing of audit reports, and leading change to produce their clients’ SOC 2 and SOC 3 compliance reports internally. “It [was] a change that impacted the whole organization,” he explains. “There was not a structured approach in place to do these audits so, from that perspective it was a significant change because it is going to be repeatable and reusable.”

Executive support

From the beginning, Bhatia stresses, there must be buy-in from the highest level. “I had to confirm that buy-in is there and in my case I was lucky that buy-in was already there, that executives were looking for this change—so for me, it was pretty smooth.”

Building Blocks of High-Quality Change

“The building-blocks approach to change management is designed to drive positive change through people rather than driving people through a change. The 10 building blocks combine strategic elements with transactional tools and methodologies, interacting with and reinforcing each other.”

Source: Addressing the change constant: Successful change from the inside—PwC, 2012, ©PwC

Aligning partners

Enlisting the right partners was also crucial. “We had a really experienced couple of companies we were working with.” From them, Bhatia says he was able to set expectations and get expert guidance in the preplanning needed. “The whole process was laid out in a way that we could flow smoothly. Because we did a gap analysis ahead of time…we did not have any hiccups.”

Employee buy-in

Gaining support from the employees takes patience and detailed communication. “You have to communicate why you are doing this,” Bhatia asserts, “and what the organizational incentive and the business reason behind [it are] so that is understood by all the stakeholders.”

Through regular communication, they shared details, schedules and expectations. “Most of the stakeholders understood. There were some that needed clarification and it was just one-on-one meetings to sit and explain…. Luckily, I have stakeholders within the company that were very fine with the expectations.”

The project was a success, and Bhatia says a lot of the credit goes to the people who made it happen. “I have a lot of experience in corporate America and our partners had a lot of experience and our internal stakeholders had a lot of experience. So the maturity level was very high for all parties involved and that made a huge difference.” How big a difference? “The main success factor in my case was that we picked the right team.”

The success is paying dividends for Bhatia’s company.
“The framework that is in place can now be reused at a much lower cost [and is] a more seamless experience for the people involved.”

**TROUBLE AHEAD—KNOW THE WARNING SIGNS**

The project is underway; the plan, requirements and timeline have been communicated to all involved. But there are potential curves and bumps in the road. Knowing what they might be and how to react are crucial to success.

**Leadership Disengagement**

“More often than not, leaders will say, ‘We’re going to do this,’ then delegate it down to their leaders who then delegate it down.” That, PwC’s Cusumano says, is a recipe for failure. Consultant Ashkenas agrees: “The CEO needs to really own [the project]. The CEO cannot say, ‘My IT guy, or my head of security said we’ve got to do this. I don’t understand it, but I want you all to do whatever he tells you to do.’ That can’t be the message. It’s got to be, ‘This is an imperative for our business.’”

La Piana recommends engaging a senior manager to whom you can bring these concerns and who can get you time with the CEO. Ashkenas also supports having a small team to act as sponsor. “The CIO should have a little business advisory team…so it’s not just seen as an IT project.”

Holding all the stakeholders accountable for their part in the project is a necessity for success. A regular review process will keep everyone on track, suggests Ashkenas. “Maybe it’s part of a weekly staff meeting...or once a month at a minimum to say ‘What’s our progress?’”

**Second thoughts**

“Most executives want the outcome, they don’t necessarily want to do the work,” says Cusumano, “because it’s less tangible how that process contributes to the ROI,” she explains. ‘Well, how many resources need to be dedicated to it? What does the work entail?’ Those are the issues you confront…but you have to get them over the hump of why this is important.”

She warns that it takes patience and strength to re-engage leadership. “Be empowered, and find ways to engage your leaders in meaningful ways which let them understand what people really think about the change and the kinds of questions [they have].” She recommends “face time” between the CEO and those working on the change as a potential remedy. “Throw a brown bag [lunch] and ask the leader to participate. Get with that leader a couple of days before and talk about, ‘Here are the things our people need to hear.’”

**Too much, too soon**

Bhatia urges caution when the timetable looks tight. “You know the leadership wants to put the change in very fast and you think that it’s not doable given the current priorities.” He advises having a good understanding of the internal and external markets’ readiness for change. “The organization is not ready for the change...[if] the stakeholders are not fully provided the time and resources.”

**The Roadmap to Success**

Whether the management for the organization’s change falls to the CIO, CSO, CISO or an external project management organization, successful change requires planning, persistence and passion. Some key components to that roadmap include vision and support from top leadership, buy-in from all those engaged in making the change happen, and constant communication, problem-solving and accountability at all levels. With all of that, the odds for success should be ever in your favor.

DEBORAH JOHNSON is managing editor of InfoSecurity Professional.
BUSINESSES EVERYWHERE ARE undergoing a digital revolution. Executives are fully embracing the potential of more digitized corporate and consumer worlds, from deeper investments into e-commerce, to virtual servers and cloud-based technologies. But this revolution is also taking place amid growing exposure to risks, specifically cyber risks. In the best case, the aversion to these risks results in a new business model being delayed; in the worst case, the parallel (bimodal) “digital” structures are set up with no controls related to risks.

A digital transformation brings a higher level of agility vital to an organization’s growth. Yet, information security is more often associated with rigidity rather than agility. We cybersecurity professionals tend to proceed more slowly—and definitively slower than our business associates when it comes to adopting new technologies, let alone transforming an entire organization.
Aspiring to be a CISSP? Get Your Free Planning Kit.

CISSP is the most globally recognized certification in the information security market. It’s also known to be a rigorous certification exam, so preparing for it can be overwhelming.

(ISC)² is here to help guide you, starting with our free CISSP Planning Kit.

Your kit includes:
» Fast facts about CISSP
» An overview of the CISSP exam
» Your success roadmap (aka planning and study tips)
» 5 tips to help you maintain your CISSP certification
» 22 continuing education ideas

Download your free kit!
In between the agility of digital transformation and the rigidity of security, there is a narrow space for the path forward. This path is both methodical and pragmatic. It identifies and mitigates existing and future risks in the most exhaustive way, while allowing digital innovation to take place.

Here’s how we can all move forward, safely and securely.

**ANTICIPATING RISKS: IT’S WHAT WE DO**

As an organization adopts digital platforms, from cloud-based services, to big data analytics, to extended use of mobile for workforces, it’s important to address risks as they come up (or even before)—not after the process is complete. Many solutions currently address specific current and future risks, but unfortunately it can be difficult when digital is still in the experimental stage with so many unknowns. At best, the “sketch” of the final picture is just being drawn. Due to the confidentiality of digital strategies, the communication of this sketch is also limited or nonexistent. It makes it difficult to attach security requirements to a moving target.

The challenge is how to protect the existing “legacy” information assets, while at the same time allowing the new digital initiatives to evolve and develop, with limited constraints to mitigate threats.

At the outset, it’s important to understand the stakes involved in a digital transformation. Therefore, knowing each organization’s (business) unique environment is crucial.

**BUSINESS FACETS OF THE DIGITAL TRANSFORMATION**

Digital transformations take many forms, but have at least one thing in common: they are done to gain a competitive advantage. They create more efficient business operations, while also creating new headaches for cybersecurity professionals. Here are just a few challenges some industries face as they move toward a more digitized consumer world:

**Insurance**

Use of connected, internet-enabled networks now allow on-demand insurance contracts based on a pay-per-use model.

*Challenge: How to protect all of the data transferred and collected?*

**Pharma**

Use of mobile applications and big data to establish a direct link with a patient or provider, to transform the industry value chain.

*Challenge: Staying on the right side of regulatory compliance.*

**Banking**

The increased popularity of digitalizing financial contracts (such as for home and auto lending) that use digital signatures.

*Challenge: Legal compliance and secure archiving.*

Improved customer experiences (and remote banking options) with more digital interaction using mobile devices, particularly smartphones and tablets

*Challenge: Accessing highly sensitive data using public Wi-Fi with potentially extended access rights granted to clients.*

**Utilities**

These companies often are at increased safety risk during maintenance operations in exposed environments (nuclear). The use of mobile devices and augmented reality may decrease exposure of employees to safety risks.

*Challenge: Securing the mobile devices accessing core information systems.*

**INTERNAL FACETS OF DIGITAL TRANSFORMATIONS**

There are the business aspects of a digital transformation, and then there are the internal changes organizations undergo while introducing new devices, infrastructures and associated use cases. It can be superficial or it can go so deep that it creates a revolutionary shift within the company culture. Such a transformation strongly impacts human resources, which is why a key element of any digital plan should including working with an HR department to provide security awareness as it relates to these new use cases.

Some examples include:

- Collaboration facilitated by introducing private and public social networks.
- Field operations facilitated by mobile devices and extended accessibility of information systems from outside.
BYOD policies that mix personal and professional use of mobile devices.
- Cloud workplace solutions that provide on-demand access to data from everywhere.
- Multi- or omni-channel communications.

Each organization must master four key technologies in order for digital transformation not only to work as intended, but to protect sensitive data in the process. They are: mobile devices, cloud computing, big data and the Internet of Things (IoT). Very often, each of these areas are addressed separately from risk and security perspectives. However, some common traits allow a holistic approach for security during a digital transformation.

So, what key capabilities should you develop to keep better control of the risks that arise in a digital era?

We all know there is no such thing as zero risk or 100 percent security. It is impossible to cover all the risks even though they should be considered with a holistic view. A more pragmatic approach may consist of co-operating a “fix the basics” program focused on protection of existing assets and a “digital security” program that targets new requirements for emerging digital technologies and solutions, now or eventually built for an organization.

**FIX THE BASICS: ALIGNMENT WITH BUSINESS RISK MANAGEMENT**
Every organization must provide some level of protection to existing assets in order to conduct business securely. This includes:
- Protecting assets based on their value to the business.
- Deciding what controls to implement based on a hierarchy of those business assets.

There’s also a solid basis to build excellent security operations—as any operational cybersecurity activity and protections to mitigate threats will take into account any impact on the business.

**FIX THE BASICS: OPERATIONAL EXCELLENCE IN SECURITY**
On the operational side of cybersecurity, this risk-based approach translates into considering the business impact of risks, rather than IT impact. For example, a Security Operation Center demonstrates its added value to the business by protecting its most valuable assets and providing means of efficient data leak prevention.

The security systems were built by successively adding tools and controls over years. Therefore, continual system optimization seems necessary. It takes into account the cost and the added value of each component to get the right security at the right price. Also, the security processes can be optimized with lean techniques.

Digital conversion or adoption covers multiple topics: cloud, mobile, big data and IoT, just to mention the most common forms. Each presents some specific risks.

**THREE KEY CAPABILITIES TO SUPPORT THE DIGITAL**
Data is often referred to as the “new gold” of the digital revolution. Data is an asset, and an asset is an object characterized by a value. This is the reason why data is being stolen and why it needs protection. Sharing such assets enriches the data and adds value. Understanding the central role of data in the digital transformation leads to three important security capabilities to develop, expand or refine in the coming years:
- Share and control—capability to share data and to control who has access to it
- Close protection—protection focused on data (as opposed to perimeter) and close to the data
- Trust technologies—new security technologies allowing to build trust and introduce new business models

Let’s further examine each.
SHARE AND CONTROL

It is commonly agreed nowadays that data (or information) has value. The information is an intangible asset; it is a set of data stored in a system. The value of information comes from the knowledge gained from it. This transfer can be controlled by the owner in two ways: (1) by deciding what are the channels used to share the information and (2) by deciding who can access the information.

Sharing information creates value: the data can be sold; the data can be acquired; and internal and external data can be correlated to create value (increase value of data). This data sharing implies the mastery of not only classic interoperability and newer cloud technologies, but also an increased ability to control the access to the shared data. Sharing of an increased amount of internal data with external partners will require ways to manage external identities, including possibly using identity federation. Also identity control itself will have to be increased, such as using strong authentication, as more and more critical data is accessible from outside.

CLOSE PROTECTION

The IoT associated with big data leads to exponentially more data being collected and processed. At the same time, the data is also increasingly stored and accessed through mobile devices, rendering classic perimeter protection strategies inefficient. The protection approach will have to evolve and get closer to the actual data regardless of its structured (in a system) or unstructured form.

Furthermore, as companies expand and globalize, data protection becomes a compliance issue with strong pressures from regulatory bodies worldwide. The recent data breach scandals also highlight how quickly client trust can evaporate when a company’s poor data protection is made public.

TRUST TECHNOLOGIES

Trust is a fundamental characteristic of any business activity. Consider a nation’s currency, which initially involved citizens placing trust in a new system—a central bank—before such a monetary system was widely accepted. Then came the banking industry, which had to convince customers their money was safer deposited with them than in a secret hiding place at home.

Many current and emerging information security technologies provide ways to build trust in the digital world. Some common tools security professionals can use to build trust and also show value to an organization include digital signature and legal archiving, digital rights management, Blockchain, digital DNA, RFID and more.

Despite all of the advances made in recent years, there still is a “digital divide” among businesses operating on a national or global scale. That gap, however, is narrowing as more companies, small businesses and governments take the plunge and dive into replacing physical structures and analog technologies with digital ones. Such digital transformations also touch market leaders, as they need to transform their business and interaction with their clients to better defend their positions from new entrants employing disruptive strategies.

Such transformations would require careful planning and caution, but the business cannot wait because very often it is a question of its own survival. By understanding what is at stake during a transformation, risks can be anticipated—that’s where a security team can prove its worth. Not only does it raise security’s profile and value within an organization, it can also save its future reputation as those digital assets gain value and, as such, more attention from cybercriminals.

CISOs and other security executives and managers have an opportunity to help business leaders understand the risks that accompany a world that is going to be digital, whether you are ready or not. So, it’s best to control current risks and anticipate the future ones.

ADAM WOJNICKI, CISSP, is senior partner for the CIO Advisory at Sia Partners in Paris, France.
Today’s employees are asked to do more tasks in less time than ever before. Software is continually changing to meet these demands, addressing bottlenecks and freeing companies to focus on their core competencies.

And then there are IT policies. We’ve figured out how to take most of those binders of paper policies and digitize them, and even how to slice and deliver them electronically to employees in smaller, more targeted packages. But in the process we haven’t figured out how to reduce their size or number; in fact, we probably have added more policies to keep up with the growing number of regulations with which companies are required to comply.

FIGURE 1 (right) outlines considerations for different elements of policymaking.
Like laws, you don't want your employees to learn about policies by violating them. So how do you go about getting them to your employees when they need them? And how do you train on them in a way that sticks?

RETHINK YOUR DEFINITION

In the past 15 or so years, I have become very good at policy writing. This is because, as soon as people figured out that I was able to write one IT policy, it became my job to write all of the IT policies.

It can be difficult to know where to start, especially if you are new to policy writing or if an auditor or manager is waiting for you to finish writing something new. The process of policy writing might be easier if your company has a template to use; however, the next step—whether you use a template or create one—is still to get the policy to your authorized users.

We don't write detailed policies for them to be read and then collect dust. Or worse, to collect dust without being read in the first place. Ideally, we want those policies in front of our employees every day, where they have ready access to them. The big question is: Who needs to know what and when?

First, we need to sweep away our preconceived notions about what a “policy” looks like. In the past, we detailed out the types of documents that we needed. Please keep in mind: the “policy” is actually not a document; rather, the “policy” is what we are allowed or not allowed to do in a given company. Once we focus on the actual rules and requirements instead of the documents themselves, we can begin to define the who, what and when.

Fortunately for today’s IT policy writers, there are several frameworks and standards (such as ISO27k, COBIT, NIST, PCI, HIPAA and GLBA) that can assist with identifying the policies that an organization needs to have in place. It is not a requirement that policy writers read through all available frameworks and standards; however, as a policy writer you should at least be familiar enough with them to know how they apply, if at all, to your organization.

Start by listing high-level policy requirements and the regulations they address, whether internal or external. This can simply be “the building and designated areas must be secured from unauthorized entry” or “all sensitive data must be protected.” Here’s where a read-through of the frameworks and standards can be most helpful.

THINK ABOUT YOUR AUDIENCE

Define your audience before writing (or revising) your policies. Each of the document types in Figure 1 (p. 25) are generally for different audiences. For example, a Process document is typically written for management, auditors and others who need to see the “big picture” of what is to be accomplished. The audience for a Work Instructions document is the worker whose job it is to perform the task. While the audience for the Process document probably cares about a “Purpose” section, this section is redundant for Work Instructions.

You don’t want to leave it up to the reader to make inferences as to what parts of a policy, or which policies, apply to them.

Providing clarity and direction to the employees is crucial in a policy document. A “one-size-fits-all” approach can be confusing, while many different versions of the same document can be just as confusing and costly. You don’t want to leave it up to the reader to make inferences as to what parts of a policy, or which policies, apply to them. Rather, try using a table to identify the part(s) of the policy, procedure, etc., relevant to each type of audience.

For example, a decision matrix on when to use the change management procedure could include network scenarios, application scenarios, telecom scenarios, etc. Each of these audiences would use the same change management procedure for their own scenarios described within the matrix.

STREAMLINING YOUR POLICIES AND PROCEDURES

If you have both policies and procedural or work instruction documents, consider combining them and adding interactive documents such as forms. Your change management form could be created in your HelpDesk system as a template with a sequence of steps with user input. In the headings or descriptions for each step, the policy requirements could be added, such as: “Approval Signature: You must have this change approved by your manager before you move on to the next step.”

If you can add all of your policy requirements to the form, your change management policy, procedure and work instructions could amount to one decision matrix and one
form in total. If that form is included inside a HelpDesk ticket, the testing evidence, approvals, etc., could also be captured on the ticket (or attached) as well.

**FINAL WORD ABOUT TRAINING**

One of the things that drives process improvement is a user’s natural inclination to question why things are set up and carried out the way they are. Regular training is the perfect opportunity to provide a background and purpose for your policies, procedures, etc., especially if they are combined. For successful training sessions, consider the following recommendations:

- **Schedule training sessions multiple times a year** to accommodate changes and new users.
- **Make your training sessions interactive** with a live trainer. Use the internet for remote sessions. A live trainer can give more detail, take questions, explain why some alternate solutions did not work and increase buy-in.
- **Provide lunch.** Most users have full schedules but can sit for an hour of training at lunchtime and would rather have lunch with you than read extra pages of explanation in a document. This also shows that you are willing to work around participants’ schedules.
- **Create fake situations with real people.** Calling people out on mistakes or putting them on the spot to answer questions about something they just learned can create a negative impression. Assigning a participant to be in a pretend situation to illustrate a point can heighten understanding and increase retention of the material.
- **Ask participants how you can improve.** Tell them, we put this part of the policy here because we want you to know this whenever you do that. Ask them, is our strategy working?

Not every policy, procedure, etc. will be a candidate for consolidation, such as policies designed for specific audiences or regulations. However, if you take the time to tailor your documents toward your audience’s usage requirements, you’ll not only make it easier on them, but on you as the writer as well.

**KAREN CHAMBERLAIN, CISSP, has written and reviewed IT policies for 15 years. Her first experience with policy writing came while working at a company trying to become ISO 9000-compliant.**

---

**SITUATION** A company has a 10-page PLC (SDLC) policy that details the phases and expectations for three types of projects: small, medium and large. A separate PLC procedural document is six pages. Templates, mostly in Word, exist for each of the deliverable documents. For each project, folders are created on an intranet site, and deliverables are placed in the appropriate folders. Some templates are not needed and therefore missing for some projects. A project plan is maintained in MS Project.

**POSSIBLE SOLUTION**

Create a new Excel workbook. On the third tab, first column, enter the project phases, one per row. In the second column, enter the procedural steps for a small project for each phase (all steps in one cell). In the third column, enter the deliverables needed for each phase (*can denote mandatory). In the fourth column, enter the alternate options and/or notes. Repeat for medium and large projects, each on their own tab (fourth and fifth tabs). Discard existing PLC procedural document.

On the sixth tab, place the first template. On the seventh tab, place the second template, etc. Repeat until each template is on its own tab. Remove sections such as Purpose, Objectives, etc. and keep only the fields that are required to be completed for the project. Give policy and other guidance on required fields. Auto-populate similar fields on multiple tabs. Discard all separate template documents.

Review the PLC policy document and add those policy elements to the second tab that are not defined already on any of the other tabs. You may include references to other tabs if necessary, but your policy should only be a few paragraphs at most.

Add new requirements for new projects to use the workbook, retaining either the third, fourth or fifth tab, whichever is appropriate, and requiring “N/A” at the top of any template not required.

Add a legend to the first tab. Rename all tabs. Remove the requirement for multiple folders for the project—you will have only a project plan, the Excel workbook, approval emails and testing evidence to post on the intranet site. The project manager will be able to review the workbook to assist with assessing progress for the project plan. 

---

Even if you don’t adopt this methodology, the example below might get you thinking about how you can improve upon your own policies.
DURING A RECENT trip to Portugal for a conference, I was issued a hotel room key to do everything from activate the room’s electricity, to turn off its lighting.

I was there for a conference and, due to the day’s activities and jet lag, I fell fast asleep that evening. Hours later the phone rang with my prearranged wake-up call, but I fell back asleep right after figuring out how to stop the ringing. Then came a hard knock at the door. I opened it to find a uniformed hotel employee who told me, “Mr. Nusz, you missed your wake-up call.”
Once assured I was still alive, he left and I went back to sleep. Then came a second knock from another hotel employee, this time informing me my telephone was off the hook and it was his job to check it out.

This particular brand of customer service could easily be construed as an invasion of privacy. But it also serves as a metaphor for the rude awakening that’s coming May 25, 2018, when the European Union’s General Data Protection Regulation (GDPR) takes effect. The sweeping legislation could change the way companies do business, both within and outside EU nations, and will impact those security and privacy professionals who may have to protect data differently to keep regulators at bay.

EU legislators have long wanted to protect the privacy data of its citizens no matter where their data is processed or stored. Several years ago the EU started working on regulation with teeth to replace the European Union Privacy Directive of 1995. This was started before Safe Harbor, enacted in 2001, because the United States was seen as having insufficient privacy laws to protect EU citizens’ data.

The GDPR mandates safeguards be in place to protect any EU citizens’ privacy data that is transmitted, collected or stored (including in or to the U.S.). Penalties for violations can be stiff, and although this statement is not a complete review of the violations, they could amount to 4 percent of worldwide gross sales for the previous year among offenders, per Articles 83(4) and 83(5). The latter, Article 83(5c), applies to several situations, including the transfers of personal data to a recipient in a third country, or an international organization pursuant to Articles 44-49.

SIGN OF AN ALREADY CHANGING PRIVACY CULTURE IN THE U.S.

It appears that GDPR, approved in April 2016, may have already started influencing the culture of privacy in the U.S. On Oct. 27, 2016, FCC leadership voted 3-2 to require, among other items, an opt-in for customers of broadband providers to allow them to use and share sensitive information, including precise geolocation data, financial information, health information, children’s information, Social Security Numbers, web browsing history, app usage history and the content of communications. Broadband providers will have a year to comply after the rules are published.

WHO WILL NEED TO BE COMPLIANT—AND HOW?

If you are sending EU citizens’ privacy data to the U.S., or storing their privacy data from their visits to your website (IP addresses will be considered privacy data), you will be subject to the EU General Data Protection Regulation by May 25, 2018.

If you have any questions about whether your company will be subject to the new regulation, consult legal counsel soon, so you are ready to prepare to meet new rules when they go into full effect.

Some of the new privacy requirements include the following:

- Privacy Impact Assessments (officially known as Data Protection Impact Assessments)
- “Privacy (and Security) by Default and by Design”
- Report of a data breach within 72 hours—or explain why that cannot be done
- New rules regarding data access: No longer is it appropriate, regarding privacy data, to give Read access to everyone because integrity was the primary objective
- During system testing, determine when copies of production data require masking or encryption of privacy data
- Specific and detailed documentation of policies, procedures, processes, risks and controls to protect privacy data, including for cloud service providers
- Data flows of privacy data will need to be mapped
- Evidence of compliance will need to be available upon demand
- Data Protection Officers (DPOs)—These are professionals hired by the company and involved in all processes, but who report to the Supervisory Authority
- Right to Erasure (Right to be Forgotten)

All of these requirements, and others, apply to “Controllers” (the companies that own the data) and their “Processors” (service providers).

WHAT ARE THE PENALTIES FOR NONCOMPLIANCE?

The penalties can be up to 4 percent of worldwide gross sales, per Articles 83(4) and 83(5) of the GDPR.

In addition, data subjects whose privacy data has been violated can sue.

A privacy professional in a Fortune 30 global firm recently shared with me a concern that others most likely consider a risk too. What happens when a Data Protection Authority representative in one country where the firm does business visits a smaller office within a jurisdiction, but without a privacy or security professional present at the time of an unplanned visit? The DPO’s demand for proof of GDPR compliance may catch staff off guard and lead to a considerable fine.
The controls needed to prevent this risk include extensive and thorough training, education and awareness; designating appropriate privacy representatives in all offices; and to have communicated a companywide, consistent privacy message that employees know, and have practiced.

WHAT IS NEEDED TO COMPLY?
As a major part of my job, I have assisted companies in achieving compliance with both Sarbanes-Oxley and the Payment Card Industry Data Security Standard. By contrast, GDPR appears to be much more involved than both of those U.S. regulations combined.

Achieving compliance will take the realization and understanding of what GDPR entails, executive management support, a gap assessment, and a roadmap supported by sufficient money and other resources to see the program through to implementation and maintenance. It will likely take, for many companies involved, all or most of the two years companies have to achieve this.

PRIVACY IMPACT ASSESSMENTS (DATA PROTECTION IMPACT ASSESSMENTS)
An important initial step is to conduct Privacy Impact Assessments, which are, at their essence, assessing risks to data subjects’ privacy data.

Article 35 addresses Data Protection Impact Assessments, or Privacy Impact Assessments:
1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the Data Protection Officer…

To do it right means that you know, at a minimum:
1. The significance of the privacy data in the new process or system, or in the system or process being changed.
2. Where that data is.
3. How, when, and where that data will be processed, and why, and by whom. A Privacy Inventory should be created if it doesn’t already exist, and be maintained in the course of performing Privacy Impact Assessments.

This will be performed mostly in projects (new systems/processes, and modification of existing systems/processes), by the project team utilizing the processes and templates provided to them, and reviewed and approved at selected Gate/Management Reviews.

Each Privacy Impact Assessment will include per Article 35(7):
1. A systematic description of the processing operations and their purposes
2. An assessment of the necessity and proportionality of the processing operations in relation to the purposes
3. An assessment of the risks to the rights and freedoms of data subjects…
4. The measures needed to address the risks, including safeguards security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

It is important to build in controls that prevent, detect, and correct the risks.

In addition, Article 36 requires the following:
1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk…

RIGHT TO BE FORGOTTEN
One particular element of GDPR that must be factored into these assessments is the right to erasure, or the right to be forgotten.

Article 17 says, “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies.” Those conditions are beyond the scope of this article, but consider this one situation, given its breadth, “Where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.” In other words, once a transaction is complete, the consumer has the right to have their privacy data deleted from any databases.

Overall, a responsible position is to perform a Privacy Impact Assessment in conjunction with a Security Risk Assessment whenever there’s a new processes or system introduced, or one that changes how privacy data is treated. After performing these assessments, it’s important to remediate and to securely store for easy retrieval.

Privacy Impact Assessments are similar to Security Risk Assessments.
Assessments in that they are there to assess risks, apply the appropriate controls, and then assess the residual risk. IT security generally relies on project teams to perform the initial assessment. The Privacy Department can do that as well. This is done by providing questions in templates for the project teams to complete whenever systems and processes are being modified. Privacy should get involved where sensitive privacy data is involved.

REMEMBER, IT’S ABOUT IMPACT

Remember, it is a Privacy Impact Assessment. That should quickly remind us of the Business Impact Assessment or Analysis document, which should be done annually or whenever a major change occurs to help prepare for the Disaster Recovery and Business Continuity Plans. The results of this Privacy Impact Assessment should also inform the Business Impact Analyses, which will also likely be required upon request with the GDPR. Additionally, these documents are utilized in the analysis phase of Incident Response, when they are available. One of the first questions that arises in Incident Response is what is the potential impact from this incident, based on the data involved, particularly if the data is sensitive data? If that information is not available, another method must be utilized to estimate that impact. The Business Impact Analysis Document should also be initially updated in a project, and then reviewed in more detail at a later time. That is how Privacy Impact Assessments are different, in that they also measure the impact should those data elements be misused, or involved in a breach or violation.

This is a good time to mention that it will be critical to categorize your privacy data, from the least to the most sensitive. Many companies, to my understanding, have not implemented data classification, and some for good reasons. However, privacy data, if nothing else, should be categorized, and policies and procedures should be developed and implemented around those categories of privacy data, with appropriate controls.

OTHER OBJECTIVES

Other objectives that can be furthered during the preparation and review of the Privacy Impact Assessment are the following:

1. Data flows: The life cycle of privacy data involved in the system should be diagramed and understood.
2. Data minimization: To minimize breaches, require as little data as possible be utilized, which also will be key to reducing the risk of GDPR violations.

Now we move to look at the function and requirements...
of the Data Protection Officer (DPO).

THE DATA PROTECTION OFFICER
A Data Protection Officer will be required under this regulation. The individual filling this position will be expected to have an excellent command of both security and privacy. The DPO will be involved in setting up policies, reviewing Privacy Impact Assessments, and all other important processes involved in complying with this regulation.

However, unlike almost all other significant positions, management cannot fire the DPO since that person reports directly to a Supervisory Authority. Such professionals are now required, and at times outsourced, in Germany. The GDPR is expected to create, outside of government entities, some 24,000 DPOs!

Specifically within the regulation, Article 38 provides the following rules for companies and their Data Protection Officers:

1. The controller and the processor shall ensure that the DPO is involved properly and in a timely manner, in all issues that relate to the protection of personal data.
2. The controller and processor shall support the DPO in performing the tasks...by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. The controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The DPO shall directly report to the highest management level of the controller or the processor.
4. Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
5. The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
6. The DPO may fulfill other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

According to Article 39:
1. The DPO shall have at least the following tasks:
   a. To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
   b. To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and the related audits;
   c. To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 (Data protection Impact Assessment);
   d. To cooperate with the Supervisory authority;
   e. To act as the contact point for the supervisory authority on issues relating to processing including the prior consultation referred to in Article 36 and to consult, where appropriate with regard to any other matter.

2. The DPO shall, in the performance of his or her tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

CHANGE IS ON THE HORIZON... PERHAPS ALREADY HERE
The EU’s General Data Protection Regulation is poised to have a huge impact, not just in Europe, but well beyond the region. With it will be a huge culture change for any company subject to compliance. It will require commitment, executive management support, assessment, planning, execution and monitoring.

It also will create new responsibilities, positions and terms of use for how companies handle consumer data. Additionally, GDPR will establish a new breed of security and privacy professional, the Data Protection Officer, who will monitor for compliance and be hired by a company, but report to an independent authority.

Some companies are already well into their Privacy Impact Assessments, while others only now realize something needs to be done. Regardless of your organization’s chosen course of action, one thing is clear: Everyone is going to be handling privacy data differently 18 months from now.

HARVEY NUSZ, CISSP, CIPM, CISA, CRISC, is a Privacy Shield and GDPR Program Manager and Consultant for a Texas-based company.
What a Difference a Year Makes
2016 marked by record-breaking survey, scholars and Garfield

IT WAS A YEAR AGO that we began the transition from the (ISC)² Foundation to the new Center for Cyber Safety and Education. But we did more than change our name; we made great improvements in all three of our core focus areas: research, scholarships and education.

In the March/April issue you will begin to see the results of the revamped 2017 Global Information Security Workforce Study. Early in 2016, before we launched the survey, we gathered a team of security experts, staff, marketing and research specialists for two days to comb through every question of the previous survey. We knew (from your feedback) that the last survey was too time-consuming and needed to be shortened.

We realized some questions had veered from our central goal of focusing on the workforce. So some questions were eliminated, and others revised. With the help of the Executive Women’s Forum (EWF) and the International Consortium of Minority Cybersecurity Professionals (ICMCP), we added new questions that would provide a more in-depth look into the current and future workforce. Our changes cut the survey time in half and resulted in a record-shattering response of 19,641 security professionals.

Findings from the new study will be released in a series of different reports throughout 2017. Gone will be the bulky printed book of information; instead, you will be able to review the data in a new interactive format on our new website www.iamcybersafe.org/research. Make sure you check the site throughout the year as new reports are released—and in a searchable format so you can access survey data, including industry salaries and budgets through the (ISC)² membership portal.

The new year also brings with it the start of scholarship season. Thanks to your support, last year we provided $150,000 in scholarships and financial aid to students around the world studying information security. We have already opened up the application process for the (ISC)² Women's Scholarships and the Raytheon Women of Security Scholarships. Soon graduate and undergraduate students will also be able to apply for financial support. Everything you need can be found at www.iamcybersafe.org/scholarships.

The other big change this past year was our new exclusive global partnership with Jim Davis and his legendary cartoon creation, Garfield, to promote the Safe and Secure Online program. The feedback from the first lesson released in October has been tremendous. The next lesson will post in January, followed by Lesson 3 in April. If you haven't taken the time to look over all the new, free educational materials for parents, seniors, and children, head over to www.SafeAndSecureOnline.org.

This is the start of another year—and one we believe will be even better for our organization, and for everyone within the (ISC)² community and beyond. ✩
Sam Goh

Sam Goh is from Singapore, where he is a senior managing consultant with IBM Security Services. He’s been an (ISC)² member for 11 years.

What was your profession before you became an information security professional?
I started out as a system analyst for Aspentech, a specialist process optimization company for the oil and gas industry, 20 years ago to implement real-time dashboard technologies for an oil refinery’s 24x7 plant operations center. I also was fortunate enough to be in the Singapore Army for two and a half years (but I can’t talk about what I did). Additionally, I worked in a couple of network operations center roles in SingTel and Primus before getting into information security.

After realizing that was your chosen path, how easy or difficult was it to gain entry?
I suppose information security wasn’t an easy or apparent career option back in the days when security was mainly a glass house protecting the mainframe and applying cryptography for network communications.

In the ’90s, I had a particularly keen interest to know how IT worked (like taking apart hardware and software, to understand how it worked). I learned how IT could change the future from reading futurist columns from Wired magazine, reading books from writers like Neal Stephenson, newsgroups like alt.2600 (where “hacking” didn’t yet have a bad connotation) and watching CSI. Although my career is nothing like fanciful CSI! The dot-com bust in the early 2000s didn’t help, but once I realized my personal interest could be a viable career path, I pursued professional competency, got into banking and earned my CISSP. I haven’t had to look back since.

What did you find most difficult about taking an (ISC)² certification examination?
It cost USD$500 back then and was a six-hour exam. I had to pass it the first time, as I couldn’t afford to retake the exam! It was a sizable out-of-pocket sum for me when I was working part-time in the day, and studying in the evening.

What is your favorite test-taking tip?
My advice has always been to trust your first instinct. You either know it, or you don’t—but don’t guess. It is OK to not know everything, but make sure you find out the correct approach to be sure of your understanding. Passing the exam is only the first step, as future clients won’t appreciate if they know you guessed your way up!

How long have you been an (ISC)² Chapter president, and what made you take on that leadership role?
It is my first year as Singapore Chapter president, and my fourth stint in the chapter since its inception. I’m one of the original founding 15 who started the chapter and have been secretary, vice-secretary, co-director and, now, president. It has been great ride so far to work with many great people, some of whom have become my lifelong friends. On this last stint, I really hope to inspire a new batch of volunteers to selflessly contribute to the growth of the chapter and the security community. It is a great feeling to know more than a dozen people at every security conference that I attend nowadays. It is true that the more you put in, the more you benefit.

What advice do you have for someone in your industry just starting a career in IT security?
Read widely. Build up a network of peers and seniors you can consult with and bounce ideas off of. Always trust your first instinct.

An expanded version of this interview will appear in the February 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
- Blogs
- Case Studies
- Content Marketing
- Custom Content
- eBooks
- Infographics
- Inspirational Quotes
- Leadership Guides
- Magazines
- Newsletters
- Press Releases
- Publications
- Social and Digital Media
- Sponsored Content
- Success Stories
- Web Content
- 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).

twirlingtigermedia.com