MORE CPE ENHANCEMENTS ON THE WAY

InfoSecurity PROFESSIONAL

(ISC)² InfoSecurity PROFESSIONAL 10 YEARS

MARCH/APRIL 2018

A Publication for the (ISC)²® Membership

EVOLVED PRIVACY

Why Non-EU Companies Face Tougher Challenges Meeting GDPR

SHUT IT DOWN NOW

A Practical Guide to Preventing Data Leakage

RACE TO THE FINISH

LAST-MINUTE TIPS TO ACHIEVE GDPR COMPLIANCE

INTRODUCING
CYBER SWITCHED
A NEW PODCAST SERIES BY (ISC)²

Escape into our new half-hour chat show during your daily commute, in your lunch hour, or while at home gardening!

Explore cyber risk impact
and its ever-growing headlines with host Adrian Davis, CISSP, Director of Cybersecurity Advocacy for (ISC)² EMEA and a special guest

Spotlight interviews
with infosec superheroes who reveal what they do and give advice to those aspiring to join the exciting world of cyber

Debate on key cybersecurity challenges
from the skills shortage and artificial intelligence (AI) to GDPR and malware

TO LISTEN AND SUBSCRIBE,

visit **www.isc2.org/News-and-Events/Podcasts/Cyber-Switched**.

(ISC)²®
CYBER SWITCHED
PODCAST

contents

VOLUME 11 • ISSUE 2

Growing mobile device and compliance demands mean companies need to have visibility and control of their business-critical data. PAGE 28

features

Cover photograph: JOHN KUCZALA Illustration above: JAKOB HINRICHS

departments

InfoSecurity Professional is produced by Twirling Tiger Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email tgaron@isc2.org.

editor's note

BY ANNE SAITA

On the Right to Be Forgotten

DURING A SECURITY CONGRESS PANEL that I moderated on the EU General Data Protection Regulation (GDPR), no component drew more questions than Article 17 on the Right to Erasure, often referred to as the "Right to be Forgotten." It gives EU data subjects the right for their personal data to be removed from certain systems without undue delay once the controller or processor no longer needs it. There are exceptions to these consumer-initiated removal requests, such as ongoing litigation, data-retention laws (think bank records that must be kept for X number of years) and certain scientific, historical or public health research.

It's no surprise this part of GDPR triggered so many raised hands; it's an area that is both complex to comply with and rife with ambiguity. It also could spell trouble for Big Tech and other companies that have long benefited from few consumer data protection laws, thus allowing a growing imbalance of power over people's private data. GDPR also requires data breaches to be reported within 72 hours of discovery. Yes, there's wiggle room in that stipulation, but I wouldn't want to be the first company to defy the mandate and end up paying millions in penalties. (And regulators will be highly incentivized to prove the legislation works by finding violators to help fund the program through substantial fines.)

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

Many, many non-EU-based organizations will be impacted by this sweeping regulation, given its global reach and that most websites track visitors—including EU citizens—for site analytics or conduct e-commerce across continents. That's why we're devoting this issue to all things GDPR (or, at least, a lot of things GDPR). GDPR experts Kevin Stoffell and Harvey Nusz provide practical advice for architecting systems to meet the May 25 deadline. Spain's Mariano Benito discusses how European companies have been preparing up to now. A trio of (ISC)² EMEA Advisory Council members explain why it's the EU pushing the world toward stronger privacy regulations—and why non-EU companies can't sit idle. Finally, U.K. member Mohammad Faheem hones in on data loss prevention, given data breaches remain a huge issue, no matter where you work—or what rules of law apply. ■

advertiser index

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

InfoSecurity PROFESSIONAL

(ISC)² MANAGEMENT TEAM

DIRECTOR, CUSTOMER EXPERIENCE
Jessica Hardy
727-493-3566 | jhardy@isc2.org

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

SENIOR MANAGER, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129 | jlefebvre@isc2.org

MANAGER, CORPORATE COMMUNICATIONS
Amanda Tarantino
727-877-2230 | atarantino@isc2.org

COMMUNICATIONS SPECIALIST
Kaity Eagle
727-683-0146 | keagle@isc2.org

MANAGER, MEDIA SERVICES
Michelle Schweitz
727-201-5770 | mschweitz@isc2.org

EVENT PLANNER
Tammy Muhtadi
727-493-4481 | tmuhtadi@isc2.org

SALES TEAM

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

REGIONAL SALES MANAGERS
Lisa O'Connell
781-460-2105 | loconnell@isc2.org

EDITORIAL ADVISORY BOARD

Kaity Eagle, (ISC)²
Jarred LeFebvre, (ISC)²
Yves Le Roux, EMEA
Cesar Olivera, Brazil and Canada

TWIRLING TIGER MEDIA EDITORIAL TEAM

EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause

Twirling Tiger™ Media (www.twirlingtigermedia.com) is certified as a Women's Business Enterprise (WBE) by the Women's Business Enterprise National Council (WBENC). This partnership reflects (ISC)²'s commitment to supplier diversity.

(ISC)²

SECURE SUMMITS / 2018

#ISC2Summits

Join the Sharpest Minds in Cybersecurity at (ISC)² Secure Summit DC

MGM NATIONAL HARBOR
D.C. METRO AREA

May 7 – 8

(ISC)² Secure Summit DC (formerly CyberSecureGov) unites the sharpest minds in cybersecurity for two days of insightful discussion, workshops and best-practices exchange. Join us and you'll walk away better equipped to tackle today's biggest cyber challenges and advance your career.

WHY ATTEND?

- Secure your place among cybersecurity leaders in government, military, industry and academia
- Gain fresh perspectives from the most experienced minds in our profession
- Earn up to 18 CPEs

Secure your place at (ISC)² Secure Summit DC.
Early bird pricing ends **MARCH 30**. Register today and save.

Register Now

Learn more about **(ISC)² Secure Summit DC** | #ISC2Summits

ENRICH. ENABLE. EXCEL.

THE LATEST FROM (ISC)²'S LEADERSHIP

executive letter

BY JESSICA HARDY

CPE Enhancements Part of Larger Focus on Professional Development

THE LEADERSHIP AT (ISC)² is always looking for ways to add value to our growing global membership. We strive to be your go-to resource for continuing education and professional development.

In recent years, you've asked us to look more closely at how members earn and report continuing professional education (CPE) credits required to maintain an (ISC)² credential. We heard you, and this quarter we will launch a new way for members to submit CPEs. This new, more modern member web portal provides a simplified process to manage your educational credits.

The first thing you'll notice is we've reduced the number of CPE-eligible categories from 16 to four:

1. Education
2. Contribution to the profession
3. Unique work experience
4. Professional development

It also will be easier to upload any needed documentation. As I write this, we're finishing up the beta launch involving 400 members, to help ensure a smooth rollout.

Jessica Hardy is director of customer experience at (ISC)². She can be reached at jhardy@isc2.org.

The CPE enhancements are part of an overarching campaign this year focused on professional development. We're making available more enriched training offerings that move beyond certification training. One recently launched pilot program provides an interactive, online, self-paced digital forensics lab that earns members four CPEs upon successful completion.

In 2018, we're also launching a career center that includes a job board exclusively for (ISC)² members. If you've already been to our new (ISC)² Community online, then you've likely seen discussions on job openings and qualified applicants in search of new opportunities. The new career center will connect employers and members through job posts, as well as serve as a resource for resumé writing, career advice and career coaching.

In 2018, we're also launching a career center that includes a job board exclusively for (ISC)² members.

You hear this often from (ISC)² leadership, but it bears repeating: We rely on your feedback to fulfill your needs as a member. This is why we provide many different outlets to hear from you. Our biennial online membership survey, most recently conducted in December 2017, sheds light on where we're doing well and where we can improve. Where needed, we will dig deeper to try to improve or replace less popular programs.

Within the (ISC)² Community, we recently launched "Inside (ISC)²," in which community members can ask questions of a featured guest from one of our regional offices or headquarters.

These programs, as well as more educational offerings coming soon, are provided because you—our members—asked for them. One recent example was our first independently-run North America Security Congress in Austin, Texas. We drew record attendance and widespread praise for those efforts. Now we want to repeat, and hopefully exceed, that success this October at Security Congress in New Orleans. With your continued feedback on what's working—and what's not—I know we can do it. ■

The

ULTIMATE GUIDES

to the Ultimate Cybersecurity

CERTIFICATIONS

CISSP® ISSAP® ISSEP® ISSMP® SSCP® CCSP® CAP® CSSLP® HCISPP®

Now available for all certifications!

Validate your expertise and show your boss you have what it takes to protect your organization with a globally recognized (ISC)² certification.

Choose which certification is right for you and download The Ultimate Guide for tips, tools and more.

Get Your Free Ultimate Guide ⓘ

These guides include:

- ✓ Fast facts of the certification
- ✓ An overview of the exam
- ✓ Benefits of the certification
- ✓ Setting yourself up for success
- ✓ Steps to getting certified

(ISC)²

field notes

A ROUNDUP OF WHAT'S HAPPENING IN (ISC)² COMMUNITIES

EDITED BY DEBORAH JOHNSON

GDPR Offers New Career Opportunities

BY MICHAEL CHRISTENSEN, CISSP, CSSLP

EVEN THOUGH information security professionals are in high demand, you can further advance your career by entering the green fields of data privacy, represented by the new EU General Data Protection Regulation (GDPR).

The GDPR has been a booster for the entire area of work. As a freelance consultant, I have experienced a significant rise in the number of requests for GDPR assistance that I receive. To take advantage of the need for GDPR experts, some suggestions:

Get certified

To be a candidate for GDPR positions coming from an information security background, I would recommend you get a certificate proving that you have structured knowledge in the area. Three recommendations are:

- GDPR-P – General Data Protection Regulation Practitioner—a very targeted course regarding the regulation, which I have.
- CIPM – Certified Information Privacy Manager
- CIPP/E – Certified Information Privacy Professional/Europe

Learn to bridge the gap

As an external consultant, I find myself in the tension zone between the legal department, IT and information security. Each has its area of expertise:

- Legal knows the regulation, but cannot put it into operation because they know little about governance.
- Information security knows about security and privacy, but needs clarification on the new set of requirements.
- IT needs governance and policies and instructions on the implementation of the GDPR's requirement for privacy "by design" and "by default."

Businesses will often look for a person who can bring together these three elements. If you can bridge the gaps, you will find yourself in some very interesting positions.

The (ISC)² EMEA GDPR Advisory Council has issued guidance on a 12-step action plan for ensuring GDPR compliance.

For the next few years, I expect a lot of activity related to GDPR—especially when the first administrative fines are issued and the grave reality hits business management. ■

MICHAEL CHRISTENSEN *is a member of the (ISC)² EMEA GDPR Task Force.*

(ISC)² Offers New CPE Initiatives

(ISC)² members now have new professional development opportunities through two new online self-paced courses.

The **UCF Compliance Mapping Certificate Course** is designed to prepare compliance mappers for the responsibility of mapping multiple authority documents correctly and accurately in a way that will satisfy auditors and regulators while simplifying governance for their organization or clients.

The **Secure IoT Networks Course** is focused on deploying IoT devices securely in your business by reducing the risk of network incursions and identifying, mitigating and isolating threats.

These new initiatives are part of (ISC)²'s mission to enhance continuing professional education (CPE) offerings that ensure members have access to affordable, relevant and quality CPE opportunities. "Our goal is to provide members with tools to help them remain competent and stay ahead of evolving trends and activities within the industry," said Stacy Mantzaris, (ISC)²'s CPE lead.

Mantzaris joined the (ISC)² education team to guide the development of initiatives that will elevate professional development offerings available to members, thereby arming them with the most up-to-date knowledge to be successful in their professional roles.

The education team at (ISC)² continues to seek opportunities to partner with organizations and curriculum developers to provide rich continuing professional education for (ISC)²'s members and other security professionals seeking to advance their careers and initiatives that ensure a safe and secure cyber world. Additional programs are in development, all designed to expand (ISC)² members' horizons.

To learn more about these courses, please visit www.enroll.isc2.org. ■

By the Numbers

High earnings of (ISC)² certification holders in a survey of 4,100 holders of the most popular 75 certifications.

Placement (out of 75)	Certification	Average U.S. Base Salary 2017
2	(ISC)² Certified Information Systems Security Professional (CISSP) Engineering	$145,940
3	(ISC)² Certified Information Systems Security Professional (CISSP) Architecture	$144,700
8	(ISC)² Certified Cloud Security Professional (CCSP)	$138,610
19	(ISC)² Certified Authorization Professional (CAP)	$131,100
20	(ISC)² Certified Information Systems Security Professional (CISSP)	$131,030

Source: *Certification Magazine – The Salary Survey 75* (Winter Edition, 2018)
http://certmag.com/salary-survey-2018-new-salary-survey-75/

TOP 10 TECH ISSUES FOR 2018 FROM MICROSOFT

1. Cybersecurity
2. Immigration
3. Technology for Rural Communities
4. Diversity and Tech
5. Privacy and Surveillance
6. AI and its Role in Society
7. Sustainability
8. Net Neutrality
9. Coding in Schools
10. Globalization of the IT Sector

https://blogs.microsoft.com/on-the-issues/2018/01/02/today-technology-top-ten-tech-issues-2018/

"...watches (both smart and basic) are on track to take the lead and are expected to grow from 61.5 million in 2017 to 149.5 million in 2021 as more vendors—particularly fashion brands—and cellular connectivity built into smartwatches help to drive growth in this category."

—IDC Forecasts Shipments of Wearable Devices to Nearly Double by 2021 – International Data Corporation (IDC)

https://www.idc.com/getdoc.jsp?containerId=prUS43408517

By year-end 2020, the banking industry will derive $1 billion in business value from the use of blockchain-based cryptocurrencies.

Source: *Top Strategic Predictions for 2018 and Beyond: Pace Yourself, for Sanity's Sake* – Gartner
https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

READ. QUIZ. EARN.
2 CPEs

Earn CPEs for Reading This Issue

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10749

Photographs: iStock

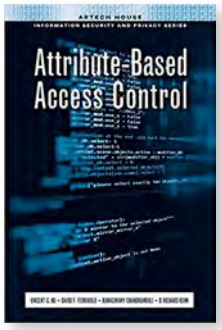
RECOMMENDED READING
Suggested by Larry Marks, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL

Attribute-Based Access Control

By Vincent C. Hu, David Ferraiolo, Ramaswamy Chandramouli and D. Richard Kuhn

(Artech House, October 31, 2017)

ATTRIBUTE-BASED ACCESS CONTROL (ABAC), the use of policies that combine user attributes rather than roles to control access to data, has been in use for several years and was published as a standard by the National Institute of Standards and Technology (NIST) in 2014.



Attribute-Based Access Control was written by the authors of the NIST standard and is a one-stop source to explaining the significance, testing and deployment of ABAC.

This book expands the standard and builds on the more than 10 ABAC models that may be relevant, such as the label-based ABAC model, and provides deployment frameworks such as XACML.

This book is geared for the security architect who is trying to fine-tune or implement a finer grade of security. The authors warn that implementing tighter access controls can be difficult and costly within ACL or RBAC models. They demonstrate how ABAC is flexible in making modifications in user authentications. Author Vincent Hu and his team address conceptual challenges and complexities that a firm will face in implementing ABAC as well as scalability, cost, decentralization and policy development at a high level. However, there is no timeline on how to negotiate the change to ABAC, and while products such as NextLabs' ABAC tool are described, there are no suggestions on how to search the marketplace for a relevant effective ABAC tool.

Attribute-Based Access Control should be supplemented with a copy of the NIST 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations and NIST 800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) for additional guidance and reference.

This book is highly recommended as a framework to successfully implement ABAC. With a clear, concise and thoughtful approach the authors outline the strengths of ABAC and role-based access control, verification and testing and other ABAC deployment frameworks. ■

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

Source: *Top Strategic Predictions for 2018 and Beyond: Pace Yourself, for Sanity's Sake* – Gartner
https://www.gartner.com/smarterwithgartner/gartner-top-strategic-predictions-for-2018-and-beyond/

US$4.03 million in lost business in 2017, up from US$3.32 million in 2016.

Source: *2017 Cost of Data Breach Study* – conducted by Ponemon Institute; sponsored by IBM Security
https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states

Photographs: iStock

#nextchapter

EDITED BY DEBORAH JOHNSON

(ISC)² BELUX CHAPTER

A New Beginning for (ISC)² in Belgium and Luxembourg

The BeLux Chapter's Security ABCs (Awareness, Behavior and Culture) event drew more than 85 infosec practitioners.

NEW ENERGY IS APPARENT in the (ISC)² BeLux (Belgium and Luxembourg) Chapter. Some members felt their chapter needed revitalizing, according to chapter president Emmanuel Nicaise. "There was a void in terms of technical continuous education in cybersecurity, in terms of promoting trust amongst cyber professionals based on their skills and values." Nicaise and fellow (ISC)² members felt that there needed to be a strong structure in place in order to share the latest knowledge. They put together a new plan for the chapter and received the official charter approval in early 2018.

The revitalized chapter has extended its outreach with new member events, including a recent conference built around the theme of "Security ABCs:" Awareness, Behavior and Culture. Eighty-five people attended with an additional eight via web conference and included presenters from the Belgian Center for Cybersecurity, the European Commission and representatives from the international bank BNP Paribas Fortis.

(ISC)² is now building strong links with other chapters in the region as well as other organizations invested in cybersecurity. "The idea is to unite and coordinate all or efforts for a greater good for the community," declares Nicaise. ■

(ISC)² BELUX CHAPTER CONTACT INFORMATION

Contact: Emmanuel Nicaise

Email: info@isc2chapter-belux.com

Website: https://www.isc2chapter-belux.com/

Q&A

EMMANUEL NICAISE, PRESIDENT, (ISC)² BELUX

The BeLux Chapter is newly chartered, yet there was an earlier chapter in place. What prompted the changes?

The earlier chapter had ceased to exist. Also, we wanted to do something different by offering more possibilities to our members to meet, to exchange information, to build trust. We aren't there yet, but it is starting. We will have our first SIG (special interest group) meeting on security awareness behavior and culture soon.

What is the reaction from the cybersecurity community to the chapter's "rebirth?"

Well, for most, it wasn't a rebirth as they weren't aware of the existence of the previous chapter. For those who were, it was a bit confusing. The feedback we have from our event surveys are excellent: 100 percent satisfaction. Of course, we still have a lot of work to do, but we have a very dynamic and skilled team of dedicated security professionals to build this community and organize these events. I have to say, organizing quality events is far from easy. So, we learned a lot and we put our hearts and sweat in it and members appreciate it.

What are the special challenges working across international boundaries?

Belgium and Luxembourg (BeLux) are small countries with a combined

population of around 12 million, amongst which around 600 are (ISC)²-certified professionals. Brussels and Luxembourg City are less than two hours' drive apart. So, international boundaries are quite relative. However, we realize that a three- or four-hour round trip might deter people from attending a two-hour event. So far, we have organized our first two events in Brussels and we are planning to organize a few in parallel in Luxembourg. We will also partner with members in Luxembourg to provide more opportunities to meet people there and to have a broader offer in cybersecurity-related events. It's a small world and we are all aiming for the same things: progress, sharing, giving back, learning, building trustful relationships. We are partnering with our colleagues from ISACA, ISSA and other security organizations to help each other. It helps to solve the "international" challenge.

The GDPR (General Data Protection Regulation) rules will take effect in May. What do you foresee as potential issues once the GDPR takes effect?

GDPR is really a hot topic at the moment—maybe even a bit too much. The good thing is that the risk of being fined for noncompliance is quite high for companies with a low level of information security management maturity. Consequently, GDPR receives a lot of attention from senior management, hence, better funding for some relevant security controls. At the same time, threats are evolving at a fast pace and cybersecurity is a continuous race between good and evil. Unfortunately, there are not enough skilled people to fill the gap between the current maturity level and the one needed to maintain a status quo. I'm still wondering how the GDPR will be enforced and what the real consequence will be as a result of the next customer data leak. Once the effect is known—after the first two or three public incidents—companies will update their risk registers and we might have some changes in priorities. Let's hope compliance won't be preferred to effective security management. ■

MUSINGS ON SECURITY ISSUES THAT IMPACT MEMBERS

advocate's corner

BY JOHN McCUMBER

Welcome to a Jam-Packed Year

THE FIRST THREE MONTHS in my new job have been a whirlwind. In my inaugural column, I outlined some initiatives I've undertaken to represent our membership and our profession. This work has not only added to my frequent flyer miles, it has also required gallons of midnight oil, and the outstanding support of the great team here at (ISC)². I owe you all a brief update.

My initial weeks here allowed me to get fully acquainted with the (ISC)² family. Yes, we call ourselves a family. I attended Security Congress 2017 in Austin, Texas, three days before my name was even on the payroll. It was followed by a meeting with the (ISC)² North American Advisory Council, and our current and future board of directors. I then spent a week at our headquarters in Clearwater, Fla., to learn about all our processes and projects, then jetted off to our offices in London while attending the Secure Summit UK event. I also sat in with the (ISC)² EMEA Advisory Council. I was honored to be on a panel of experts at the summit, and got the chance to congratulate all the winners at our first-ever EMEA Information Security Leadership Awards ceremony.

In our last issue, I mentioned our program for veterans in the commonwealth of Virginia. We are now working to replicate this successful initiative in two more states. We have also rewritten the charter for our U.S. Government Advisory Council, and are in the process of refreshing the membership and charging them with keeping us at the forefront of shaping the cybersecurity workforce for our federal government departments and agencies. I am part of a team working to bring in compelling keynote speakers and presenters for our two major events of 2018: Secure Summit DC and Security Congress 2018. They will be held at the MGM National Harbor and at the Marriott New Orleans, respectively.

John McCumber is director of cybersecurity advocacy at (ISC)². He can be reached at jmccumber@isc2.org.

Our aim is to provide you with valuable career information, cutting-edge training and, of course, those ever-important CPEs.

Speaking of these events, make sure to attend both if your schedule permits. I'm excited about the speakers we have already locked in and there will be more intriguing news coming soon. Our aim is to provide you with valuable career information, cutting-edge training and, of course, those ever-important CPEs. Most of us want to maximize our conference attendance and don't need to attend conferences full of nonsense, off-topic discussions and irrelevant sessions. You know the ones I'm talking about. We promise to not waste your time or money.

This is shaping up to be an energetic, jam-packed year. There are numerous ways you can join us as a volunteer or advisor. We'd love to hear from you! Get involved in your local chapter, start one yourself or reach out to the advisory councils in your area. In the meantime, continue to join us in the (ISC)² Community, and always feel free to reach out to me directly at jmccumber@isc2.org. ■

IT'S HERE... Almost

LAST-MINUTE TIPS FOR THOSE TRYING TO ACHIEVE GDPR COMPLIANCE ON A TIGHT DEADLINE

BY KEVIN STOFFELL AND HARVEY NUSZ

AFTER TWO YEARS OF PUBLICITY AND PREPARATION, the European Union (EU) General Data Protection Regulation (GDPR) goes into effect on May 25. By now, companies impacted by the massive legislation should have all but the finer details in place. Chances are, however, many organizations are behind, especially if they are located outside the EU and have only recently realized they must become compliant.

Make no mistake: GDPR has the potential to impact companies worldwide that collect, store and process data on EU consumers. Companies storing or processing privacy data of European citizens or residents need to ensure they are compliant or could face significant fines from the EU. The GDPR is considered an extraterritorial regulation and is inclusive of data stored offshore from the EU. Potential fines are up to four percent of worldwide gross sales based upon last year's financial statements, with a limit of €20 million.

Have we got your attention now?

The requirements are far reaching compared to what is typical in the United States, therefore they may represent a huge cultural change for many organizations.

Under GDPR, data is classified as:

Personal Data – Any information relating to an identified or identifiable natural person. Including specific references to:

- identification number
- location data
- online identifier
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Sensitive Data – GDPR prohibits the processing of personal data revealing:

- race or ethnic origin
- political opinions
- religion or beliefs
- trade-union membership
- the processing of genetic data; or
- data concerning health or sex life
- or criminal convictions or related security

Some of the requirements garnering attention include:

- Record of Processing
- Data Protection Impact Assessment
- Privacy by Design to achieve Privacy by Default
- Right to:
  - –Rectification
  - –Erasure
  - –Object
  - –Restriction
  - –Access
  - –Portability
- Consent Management
- Breach reporting within 72 hours of determining that a breach occurred that impacted data subjects. That includes breaches originating from your processor(s).

As companies currently assess their risk under GDPR, they appear to forget that this has been two years in the making, and that the EU will consider compliance to be mandatory as of the effective date of the regulation. Do not expect extensions or exceptions at this juncture.

If your company is not able to demonstrate compliance on demand by May 25, a written, funded, approved and resourced plan to achieve compliance, preferably within three months, should be in place. While many companies are working with their Internal Audit department to be able to demonstrate compliance on demand, some GRC tools are beginning to roll out their GDPR modules as well. However, delaying compliance actions until the last minute may introduce significant financial and business risk.

GDPR IMPLEMENTATION CHALLENGES

Implementing GDPR compliant IT capability, or restructuring existing IT into a compliant structure, is a daunting proposition. There are some significant challenges to technical implementations designed to support GDPR compliance.

The following describes some of the most likely and common challenges you will encounter when updating your overall architecture to support GDPR compliance. In most cases, the technical architecture will directly support or complement compliant processes or enable functionality required to meet GDPR requirements. This is a major concern when enabling effective and efficient processes related to data subjects exercising their individual rights under the GDPR.

Supporting most of the data subject rights under the GDPR requires a combination of technical function and well-defined processes that are enabled by those technical functions. While in many cases the GDPR-specified data subject rights can be accomplished using purely manual means, the effort required per data subject could be high. This can quickly become cost-prohibitive in cases where data subjects choose to exercise their rights under the GDPR frequently.

The challenges for most organizations will revolve around supporting a specific set of data subject rights. The most impactful data subject rights are:

- Article 7 – Conditions for consent: "The data subject shall have the right to withdraw his or her consent at any time."
- Article 15 – Right of access by the data subject: "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

14 STEPS FOR ACHIEVING COMPLIANCE

THE BELOW STEPS are a general set of tasks that are likely necessary for most organizations to achieve some level of GDPR compliance. Each organization desiring to achieve some level of GDPR compliance must develop a custom path that fits its business needs.

However, if your organization has not yet initiated GDPR planning, the following steps will provide a valuable starting point. If your organization maintains a comprehensive Enterprise Architecture (EA), it is likely that much of the information needed for the below steps already exists as part of the EA or can be obtained from the EA. If a comprehensive EA is not available, significant effort may be required to develop sufficient data to effectively plan for GDPR compliance and the below steps may require significant resource commitment.

1. **Conduct privacy inventory.**
Identify what privacy information you have, and where it is located in your environment. At this stage, the "where" is focused at the information system and application level.

2. **Map information to critical business processes.**
Map dependencies between access to privacy information and critical business processes to determine potential impact to business of privacy information.

3. **Determine the "value" of information.**
Determine the business value of privacy information. Determine if privacy information is truly necessary to business process and assign a valuation for the information to conduct business.

4. **Map information to technical components.**
Map the inventoried privacy information to technical components within your organization. This includes storage, servers, transmission mechanisms, etc.

5. **Identify workflows involving privacy information.**
Identify non-technical workflows that involve privacy information. These may be supported by information systems or be completely manual processes.

6. **Perform a gap assessment between current technology/workflow to GDPR requirements.**
Compare the technical components, applications, storage and workflows identified in Steps 1, 4 and 5 to GDPR requirements to determine if protections are sufficient and tools are in place to manage requirements (e.g., Right to be forgotten deletions).

7. **Conduct a cost-benefit analysis (CBA).**
Conduct a CBA that compares the costs to close gaps identified in Step 6 with privacy information valuations determined in Step 3. This will inform decisions on whether upgrading technology/process or removing privacy information is a better approach.

8. **Develop initial compliance approach.**
Develop an initial compliance approach based on Step 7 results. This may include multiple options for closing gaps or curtailing the use of privacy information.

9. **Consult legal staff/legal specialists on approach risks.**
If you have not done so, consult your legal staff or legal specialists to determine legal risk to approach options in Step 8. Ideally, your legal staff should be part of the overall process, but if they are not, ensure they are engaged at this point. Every circumstance is different and legal risk must be identified for specific cases.

10. **Conduct risk assessment.**
Conduct a risk assessment of the potential approaches and input from the legal staff.

11. **Select a final compliance approach based on risk assessment.**

12. **Implement.**
Implement the final compliance approach, monitoring effectiveness of privacy controls at each implementation phase.

13. **Assess compliance.**
Assess compliance toward GDPR requirements. This may include internal assessments and/or external assessments under the GDPR assessment programs once they are fully in place.

14. **Review.**
Continuously review compliance status. This should occur at least annually or whenever major information system or information management changes occur. ■

—KEVIN STOFFELL

without undue delay…" The full article also specifies a long list of information regarding details about data that must be disclosed upon demand.

- Article 17 – Right to erasure (Right to be forgotten): "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."
- Article 18 – Right to restriction of processing: "The data subject shall have the right to obtain from the controller restriction of processing."
- Article 20 – Right to data portability: "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."
- Article 21 – Right to object: "The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her."

This listing is a subset of the data subject rights required by the GDPR; however, it constitutes the list of rights most likely to impact the IT architecture and present definite challenges for compliance.

IDENTIFICATION AND MARKING OF IMPACTED DATA

In order to support GDPR compliance, it is critical to understand where data protected by the GDPR resides within an organization, regardless of format (e.g., electronic, paper). For electronic data, it is essential to know where within the technical architecture the data is stored, processed, viewed and transmitted.

Additionally, each data element may require metadata elements to be associated with it that associate the data element to consent or authorize types of use for the data. All data associated with a particular data subject must also be addressable in some manner that allows bulk copy or deletion of the data.

Since data subjects may retroactively restrict the use of data, IT infrastructure must support modifications to existing data structures in such a way as to allow data elements associated with a particular subject to be enabled or disabled for particular processing or usage.

NEW FUNCTIONALITY REQUIREMENTS

Any review of an existing IT architecture for GDPR compliance is likely to identify multiple areas where existing technical functions do not adequately enable efficient processes for enacting data subject rights. In many cases, data structures are not designed to selectively identify data elements associated with a particular data subject and then perform actions against all associated data elements, potentially across multiple data stores or information systems.

Similarly, there are likely instances where new data structures or functionality must be implemented in order to change processing behavior based upon data subject consent, restrictions or objections. In other circumstances, a data subject exercising the right to be forgotten may necessitate scrubbing associated data elements across multiple data structures and information systems.

Unless these functions were designed in the entire data infrastructure, they may be difficult to implement without the creation of new functionality, which may be both expensive to implement and require a lengthy implementation timeline before GDPR compliance can be achieved.

NEW MANAGEMENT AND PROCESS OVERHEAD COSTS

This challenge may require new budgetary or staffing allocations. As noted, many of the data subject rights can be executed using a manual process or with limited automation. This would likely become cost-prohibitive if data subject exercise of rights is more than minimal.

Delays in implementing technical functions to efficiently execute tasks associated with data subject rights will likely generate significant overhead costs for additional staff hours to be committed. Alternatively, if the exercise of data subject rights is expected to be low, and an organization chooses to limit new functionality or automation to support it, they may be required to implement new processes or add staff in order to service data subject exercise of rights in order to be compliant with the GDPR.

DATA USE AND REUSE LIMITATIONS

A major tenet of GDPR is the requirement for explicit consent of the data subject to be granted for many storage and processing actions. With legacy processes, this may entail a detailed review of the use and processing of all data elements against the existing consent granted by the data subject.

Information architectures will require review to ensure data elements are managed consistently with previously granted consent and within data use and reuse limitations imposed both by original consent as well as the exercise of any data subject rights that temporarily or permanently limit use of particular data elements.

A EUROPEAN'S PERSPECTIVE ON GDPR

AN (ISC)² MEMBER IN SPAIN OFFERS ADVICE TO THOSE BEHIND SCHEDULE

By Mariano J. Benito, CISSP, CISA, CISM, CGEIT, CRISC, ISO 27001-LA, BS 25999-LA

AT THE TIME OF WRITING, we were six months away from GDPR enforcement and panic was starting to set in. That anxiety is now amplified as the deadline to achieve compliance to GDPR draws near.

Most companies already approved their plans for GDPR. They procured budget months ago and are now executing these plans. Many companies already appointed Data Protection Officers (DPOs); at last count, more than 2,000 people already introduce themselves as a DPO on their LinkedIn profiles. The Data Subject concept is completely identified for personal data treatments, and risk analysis and privacy impact analysis (PIAs) have been conducted for those treatments. Although most companies have already checked that their existing security controls are good enough to address privacy risks as well, new security controls are being put into place to satisfy new, unaddressed privacy risks and/or privacy requirements.

Moreover, there is no strong need for specific awareness activities on GDPR for corporate staff and subcontractors, as GDPR has become a common topic even in non-corporate environments such as social and family, thanks partially to strong play in the news media. In spite of this, most companies are developing their own custom awareness and training programs on GDPR. They've developed materials outlining how the company will be impacted and what's changed to achieve compliance and provide accountability. Companies are reviewing their subcontracting agreements where personal data is involved in order to collect formal written data treatment agreements. This task has proven to be quite challenging in some cases, as many providers are also developing their own adaptation plans to GDPR.

The level of execution of these plans is uneven among companies, and among treatments within a company, but there is a clear path, a clear plan. There are also clear signs that companies are taking GDPR quite seriously and establishing mechanisms to raise accountability for compliance.

Nevertheless, there are other concerns ahead that need to be addressed, and adequately considered, for those companies that have fallen behind on their GPDR plan.

RESISTANCE IS FUTILE

First, many EU-based firms are still facing strong resistance to get their non-EU headquarters or subsidiaries onboard. Some of them disagree on their need to comply with this non-local regulation; some are just delaying their enrollment into GDPR due to other issues. Unfortunately, this attitude translates into a real risk for any global company, and not just for their EU subsidiaries, since sanctions are imposed based on annual worldwide "turnover" of the company.

GDPR is now IT security and privacy teams' main concern, and is creating noticeable headaches. Achieving compliance to GPDR, many now realize, is much harder than first expected. Many GPDR plans are behind schedule. GDPR implementation requires not only a plan to become compliant, but a cultural change within organizations to assure privacy for each business process, for each system, for each person. Companies need to become privacy-aware, privacy-conscious. They need to get hands-on from top to bottom in the organization in order to detect those minor unnoticed issues that went unnoticed until now. This necessary exercise requires a flexible approach, adaptive planning, and ability to find and allocate resources on demand. That's not an easy task.

Flexible planning needs to be supported with new budget allocations. As new tasks are detected and new changes are implemented and tested, budget needs to grow accordingly. Chief executives would require more reporting on budget expenditure, and they would be right, as it falls within their responsibility on when and how to comply with GDPR. In any case, it should be a risk-based decision, with the newly appointed or hired DPOs being part of these key conversations.

Finally, GDPR is not the only legal and regulatory concern for many EU companies. NIS Directive (officially, 2016/1148 Directive of July 6, 2016) concerns measures for a high common level of security of network and information systems across the European Union. Its May 9 deadline for compliance is quickly approaching, with identification of operators of essential services required by November 9. Keep calm, no need to panic: NIS's scope is narrower than GDPR, and many non-EU companies can simply ignore this regulation. Unfortunately, those who must comply now find themselves trying to comply with both regulations simultaneously. It can be done, of course, but having to meet both regulations certainly is more complicated than simply dealing with GDPR.

My balance? GPDR is now advancing at full-throttle in the eastern side of the Atlantic Ocean. The deadline for compliance is fast approaching, and its implications are not a short-term, single-shot activity. Get ready. With a comprehensive implementation plan underway and the extra budget and resources required to fulfill it, it will be worth it. ■

MARIANO J. BENITO *is CISO at GMV, an IT consultancy and Aerospatiale Spanish Corporation.*

PSEUDONYMIZATION

In GDPR terms, pseudonymization (or pseudonymisation as it appears in the regulation) means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

In more commonly used information security terms, it can be considered a form of tokenization that abstracts data elements in such a way as to obscure their actual value and source. This allows processing and analysis of data to occur in a less controlled or lower-security information infrastructure, but inherently limits the utility of data in a tokenized format. Tokenization or pseudonymization is distinct from the concept of anonymization in that they can potentially be reversed, while anonymization is a permanent action to remove data values or attribution to a particular data subject.

The GDPR presents pseudonymization as a desirable approach to limit data exposure. While the GDPR neither requires it, nor considers the use of pseudonymization by itself to be adequate as a means of protecting data, it does recommend that it be used as a protection mechanism and mentions it in multiple locations as an appropriate mechanism for safeguarding data.

APPROACHES TO GDPR COMPLIANCE

GDPR compliance is an inherently unique problem for every impacted organization. Each enterprise must assess its unique data scenario to determine the most cost-effective and lowest-risk approaches to GDPR compliance. The following presents a set of general approaches to GDPR compliance that may be leveraged to achieve the appropriate level of compliance within a realistic budget and schedule. These approaches primarily address the technical infrastructure but can also be applied to organizational structure and process.

FULLY COMPLIANT APPROACH

This general approach is to ensure the IT infrastructure and associated processes are fully compliant with GDPR protection requirements and allows for cost-effective execution of data subject rights upon demand. This approach has the highest technical costs, potentially high training costs and costs associated with ongoing assessments per the GDPR requirements.

This approach may be cost-effective for entirely new organizations or for organizations already operating in highly regulated industries. It also may be the only low-risk approach for organizations that exist primarily within the EU. While it can be employed by multinational organizations, it may be cost-prohibitive to create a fully compliant infrastructure (both IT and staff/process) for use at all multinational locations.

TARGETED ENCLAVE APPROACH

The targeted enclave approach involves the creation of compliant enclaves within the larger organizational IT infrastructure. Access to the GDPR enclaves is restricted to a subset of staff with explicit need to access the data, and information systems within the enclave are designed to easily implement functions to support exercise of data subject rights.

All GDPR-impacted data is moved into the target enclave and only stored and processed within that environment. Variations of this approach are commonly employed by organizations to protect and manage high-risk data or highly regulated data (e.g., where PCI-DSS or Sarbanes-Oxley compliance is required).

The targeted approach serves to control costs and limit risk to a defined area of the IT infrastructure and allows legacy systems and processes to continue where the costs of updating those systems or processes is prohibitive. This approach is particularly attractive for organizations that have a moderate amount of data subject to the GDPR, but very significant IT infrastructure that does not store or process GDPR-subject data.

REDUCED FUNCTIONALITY APPROACH

The reduced functionality approach involves reducing data with GDPR requirements in the organization's environment or ceasing to perform data-related operations using data covered by the GDPR.

For this approach, the value of processing or storing GDPR-covered data is weighed against the costs of GDPR compliance. If the cost-benefit analysis shows that the cost of compliance outweighs the business value, the best approach may be to cease or curtail business functions that involve GDPR-covered data.

This approach does not necessarily require a company stop doing business in the EU. However, extraneous collection, storage or secondary processing of data may not be necessary to support the primary business functions and can be reduced or eliminated to lessen compliance costs and risks associated with the GDPR's substantial fine system.

COMBINED APPROACH

In most realistic scenarios, a fully compliant infrastructure approach may be too impractical or cost-prohibitive to employ across the entire IT infrastructure of an organization. This is especially true for multinational organizations that maintain a physical presence within the EU as well as in other nations. In cases such as that, the most cost-effective approach may be to implement a fully compliant infrastructure in locations within the EU and a combination of functionality reduction and targeted compliance enclaves outside the EU.

While this likely still requires some data restructuring and moving the locations where data is stored and processed, there is significant value in isolating data elements with GDPR requirements within a fully compliant storage and processing infrastructure within the EU.

When combined with pseudonomization of data used outside of the EU, or in lower-security enclaves, a combined approach for a multinational organization will often have a net reduction in total cost while retaining similar effective functionality to a fully compliant infrastructure at all multinational locations.

Becoming GDPR compliant is not easy. That's why organizations were given two years since its official enactment to re-architect their IT infrastructure. Some may be behind, but still making progress. There are plenty of reasons why it is now or never to make GDPR compliance the chief priority and align as many resources as possible to meet the May 25 deadline.

Hopefully, the steps and options we outlined will spare you and your organization from being among the first enterprises to be found in violation, and subject to perhaps millions in fines and the loss of business once such penalties are in the headlines. ■

KEVIN STOFFELL, *CISSP-ISSAP, ISSEP, ISSMP, CISA, CEH, CSEP, PMP, is a cybersecurity architect with the Cyber Architecture and Advisory Services group at the Battelle Memorial Institute. He has more than 20 years of experience in information systems operations and information systems security in academia, military and commercial environments. He has a B.S. in computer engineering from the University of South Carolina and an M.S. in electrical engineering from the Naval Postgraduate School.*

HARVEY NUSZ, *CISSP, CIPM, CISA, CRISC, is a Houston-based Privacy Shield and GDPR expert who last year authored a three-part series on GDPR for* InfoSecurity Professional.

(ISC)²

SECURITY CONGRESS | LATIN AMERICA 2018

July 25 - 26 • Santiago, Chile

Sheraton Santiago Hotel and Convention Center

ENRICH ENABLE EXCEL

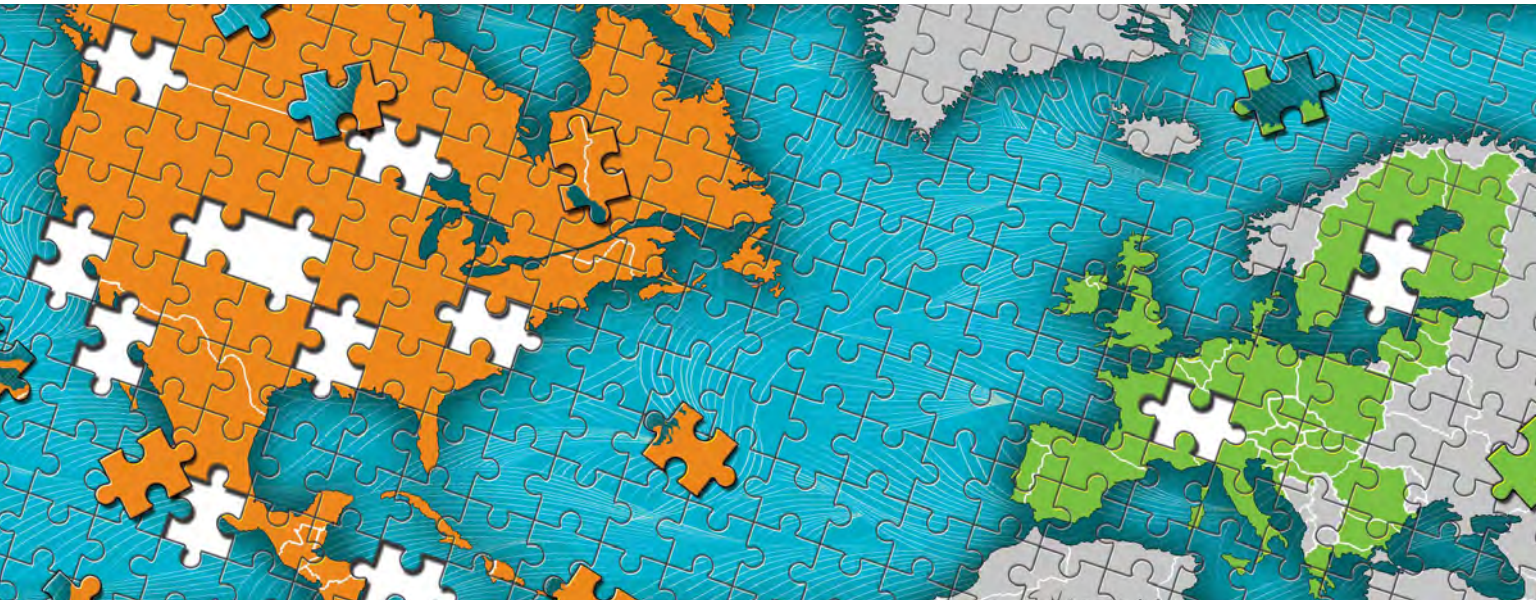
The conference of 2018 will offer educational sessions presented by international thought-leadership experts. As cyber threats and attacks continue to rise, the goal of the conference is to collaborate with the development of cybersecurity professionals, providing knowledge, tools, orientations and expertise to protect their organizations.

- Cloud Security
- Mobile Devices / Security and Management
- Gov., Regulation & Compliance
- Software Assurance, Application Security
- Malware
- Threats
- Professional Development
- Incident Response & Forensics
- Healthcare Security
- Privacy
- Identity / Access Management
- Internet of Things
- Cybercrime
- Critical Infrastructure
- People & Security

(ISC)² members can earn up to 16 CPEs • latamcongress.isc2.org • #ISC2CongressLATAM

GDPR: WHY NON-EU COMPANIES FACE TOUGHER CHALLENGES THAN THEIR EUROPEAN COUNTERPARTS

By **Yves Le Roux**, CISSP, **Paul Lanois**, SSCP, CCSK, PCIP, CIPM, CIPT, CIPP, FIP, LLM and **Visia Tartaglione**, CISSP



Three members of the (ISC)² EMEA Advisory Council's GDPR Task Force explain the evolution of EU privacy laws.

IN JULY 2016, a survey conducted at the request of the European Commission documented just how serious Europeans are about privacy, and their expectations that it should be protected as digital capability develops. More than nine in 10 respondents, for example, said it is important that personal information (pictures, contact lists, etc.) on their computer, smartphone or tablet only be accessed with their permission, and that the confidentiality of their emails and online instant messaging is also guaranteed. More than eight in 10 (82 percent) also said that tools for monitoring their activities online (such as cookies) should only be used with their permission. The majority actively take measures to protect their privacy: Six in 10 had changed privacy settings on their internet browser and 40 percent avoided certain websites because they are worried their online activities are monitored.

ILLUSTRATION BY ENRICO VARRASSO

These findings reflect a well-established respect for privacy that is not only embedded across the European Union (EU), but has also fueled a stringent regulatory environment within the EU dating back decades.

Data protection legislation in EU member countries started in the late 1970s. France was one of the first countries in Europe to enact a privacy law, after the French government secretly began working on SAFARI, a centralized database project allowing French citizens to be personally identified by different government services. A French newspaper, *Le Monde*, revealed SAFARI's existence, resulting in uproar and the creation in 1978 of France's first law on information technology, data files and civil liberty.

In October 1995, the European Parliament went on to enact the EU Directive 95/46/EC ("the Directive") to member states to enact national laws on the protection of individuals regarding processing of personal data and free movement of such data. Each EU member country applied its own interpretation of the Directive, resulting in a "patchwork" of similar, but not identical, data protection compliance requirements. It also created a significant burden for organizations with operations in more than one EU country. The European Parliament and European Council went on to adopt the General Data Protection Regulation (GDPR) to both create a unified approach to data protection across the EU, and to update the regulatory response as digital capabilities began to shape societies.

Almost as many (89 percent) agreed the default settings of their browser should stop their information from being shared.

Economic development policy led by the European Commission includes the development of a Digital Single Market (DSM), which relies on the creation of an online environment that people can truly trust. Clear rules on privacy are considered a cornerstone of the DSM.

The Commission's 2016 survey illustrates people's expectations: More than nine in 10 said that computer, smartphone or tablet providers should give them regular software updates to protect their information (93 percent) and the ability to encrypt their messages and calls. Almost as many (89 percent) agreed the default settings of their browser should stop their information from being shared. Respondents deemed it unacceptable to have their online activities monitored in exchange for unrestricted access to websites (64 percent) or for companies to share information about them without their permission (71 percent), even if it helps companies provide new services they may like.

Understanding such sentiment helps to explain some of the work that companies around the world are now grappling with as they try to meet the May 25 compliance deadline set for GDPR.

STARTING FROM SCRATCH

Many countries outside of the EU have not experienced such a long history of debate and negotiation among citizens, activists and authorities that ultimately led to stating the privacy of individuals as a fundamental right codified in law. Many will be starting from scratch, with everything from the development of new policies and processes, to much of the terminology being new to them. EU countries, by contrast, have a longstanding history of data protection authorities monitoring corporate behavior, which has influenced how companies in Europe have evolved in response to citizens' expectations.

Experience in working on GDPR compliance with companies in the United States, for example, highlights that there is still ambiguity around the simple definition of personal data. The understanding of personally identifiable information (PII) varies by industry and sometimes territory, as the U.S. does not have federal law exhaustively covering the topic, scenarios and means of handling personal data in general. There are industry-accepted standards and regulations that focus only on subsets of data, such as credit card information or individuals' health information.

It is not surprising, then, that many organizations may be overwhelmed by GDPR. The workload is not insignificant. They must build a data processing inventory, or record of processing activities, including a list of all the operations where personal data, as defined by the new European regulation, is collected, captured, processed, shared, stored and archived.

People interviewed within GDPR projects are usually not even aware that they are handling personal data. Names, last names, email addresses, electronic identification numbers—such as online identifiers (e.g., cookies), Internet Protocol (IP) and Media Access Control (MAC) addresses and RFID tags—are all personal data and are therefore in scope.

SHARPENING THE BUSINESS MODEL

Personal data is the new gold today. It is collected, captured, processed and stored for different uses, such as

business intelligence and analytics, as well as marketing previsions. The flexible and cheap availability of storage resources and the capacity of ultra-modern algorithms are naturally feeding the trend to further collect and process data, often and despite there being no strategy or plan in place around the future use. When asked, "What are you going to do with this data?" the common answer of "We do not know yet" neglects "privacy by design" principles more commonly understood in the EU. And it contrasts with the culture of purpose, awareness and limitation that GDPR aims to establish.

Organizations that have never previously enforced security by design and by default principles face having to embed privacy requirements at an organizational level and in the very early stages of projects. They need to perform assessments of the privacy impacts of relevant operations, appoint specific roles to oversee, guide and educate on privacy matters, and design solid risk management processes to identify the appropriate security technical and organizational controls required.

Organizations that have never previously enforced security by design and by default principles face having to embed privacy requirements at an organizational level and in the very early stages of projects.

Respecting the joint liability principle within GDPR is another big challenge. Typically, newly established companies in the U.S. heavily rely on cloud service providers, often encompassing hundreds of Software-as-a-Service (SaaS) suppliers and resulting in most, if not all, of their IT infrastructure being off premises. This requires the design and implementation of a selection process and vendor monitoring and management program to address compliance around transferring personal data, as the company has this responsibility along with their suppliers.

12 CRITICAL AREAS OF GDPR COMPLIANCE

(ISC)²'s EMEA Advisory Council (EAC) has established an international GDPR Task Force made up of members from around the world who are actively charged with implementing the GDPR to track and curate front-line experience with the compliance effort. The aim is to work with the global membership of (ISC)² to share the insights, tools and strategies they are deploying to meet the May 25 compliance deadline.

This task force includes members working for online retailers, finance, manufacturing, telecommunications, government and small businesses. Frequently sharing insights on the (ISC)² community and blog, it has published an action plan for GDPR compliance, highlighting 12 critical areas of activity and related tasks available at http://blog.isc2.org/files/scoping-the-compliance-task-for-gdpr---areas-of-activity.pdf.

They include:

1. Insure the support from the board and business units
2. Establish inventory of personal information held
3. Privacy notice and information
4. Individuals' rights
5. Data subjects' access requests
6. Data protection impact assessments (DPIA)
7. Consent
8. Children
9. Personal data breaches
10. Security of data processing and data protection by design
11. Data protection governance
12. International data transfers

Further, people within organizations who handle personal data must be trained to gain a solid understanding of what personal data is and embrace the privacy objectives set out by their organization so that they can become good custodians of the data.

Finally, individual rights, many of which already exist in Europe, are enshrined within GDPR, while outside the EU, the privacy of customers, website visitors and employees is often not considered or managed only as far as it concerns the liability of organizations. These rights include:

- The right of access
- The right of rectification
- The right of erasure ("right to be forgotten")
- The right to data portability
- The right to restrict the processing of their personal data
- The right to object to the processing of their personal data
- The right to object to the processing of their personal data for direct marketing purposes
- The right to not be subject to a decision based solely on automated processing, including profiling, and
- The right to launch "class actions" (with the support of a body with a statutory mandate where public interest initiates a complaint on behalf of the individual)

HOW WIDE IS THE GDPR NET?

GDPR has radically increased the reach of EU personal data protections and includes companies within and outside the EU, as long as they are processing personal data of EU citizens. It directly challenges many of the activities that are driving online trends today, such as the analysis/prediction of personal preferences, behaviors and attitudes.

A company does not have to have a presence within the EU at all to fall within the scope of GDPR. Consider a non-EU company with a global portal, a catalog with a broad range of products and services that are sourced from third parties, and which may include European languages and a currency conversion tool, and which allows personal data to be entered through this portal.

In a completely different scenario, a Turkish electronic commerce company may target Turkish-speaking customers residing in the EU (e.g., Germany), and despite its website being only written in Turkish, not an EU language, it is likely to fall under the scope of GDPR.

The legislation outlines three main questions to help companies understand whether they fall in scope:

1. **Is your company established in the EU?** This doesn't have to be a sales presence. The use of a local agent who is responsible for local debt collection and acting as a representative in administrative and judicial proceedings, and the use of a postal address and a bank account for business purposes, is considered as an EU establishment by the courts.

2. Is your non-EU established organization offering goods or services to data subjects who are in the EU? In December 2010, the Court of Justice of the European Union held that certain items of evidence, possibly in combination with one another, can demonstrate the existence of an activity "directed to" an EU member country. Factors include the international nature of the activity (such as certain tourist activities); the use of a European language; the use of a currency generally used in one or more EU member countries; the mention of telephone numbers with the international code; the use of a top-level domain name of an EU member country, for example .de or .fr; or use of neutral top-level domain names such as .com or .eu; the description of itineraries from one or more other EU member countries to the place where the service is provided; and mention of an international clientele composed of customers domiciled in various EU member countries, in particular by presentation of accounts written by such customers.

3. Is your non-EU established organization monitoring the behavior of data subjects who are in the Union? Monitoring specifically includes the tracking of individuals online to create profiles, including when they are used to make decisions to analyze/predict personal preferences, behaviors and attitudes. This includes anything that leads (or could lead) to the identification of the individual, not just personal details. For example, if an email service mines the content and metadata of each email message to target advertising for EU citizens, then it falls within the scope of GDPR.

THE DIRECTION OF TRAVEL

(ISC)²'s Advisory Council-led GDPR Task Force *(see sidebar, p. 24)* has identified a growing sentiment among non-EU companies. It appears that many have chosen a "wait-and-see attitude," thinking that GDPR enforcement may not practically reach them, rather than investing in the effort needed for compliance. The group was unanimous in considering this mindset unwise.

GDPR goes to the very heart of the business model being developed by organizations around the world, and a restructuring of operations may be needed for many organizations if they want to target EU citizens.

And there is more at stake. According to the United Nations Conference on Trade and Development, 107 countries have already put in place legislation to secure the protection of data and privacy. Many governments, specifically in developing countries, are having problems modeling their data protection frameworks, leading to most opting for an approach consistent with the EU to ensure a seamless flow of data with the EU.

For consumers, a lack of clarity regarding their protection and avenues for redress tends to aggravate their concern and motivate government action. For businesses too, while they may be concerned about rules curbing their enterprise, a lack of clarity and compatibility between regimes creates uncertainty and hinders investment. Given the nexus between cross-border e-commerce and data protection, there is growing global pressure to avoid divergent regimes as they inhibit the adoption and proliferation of emerging technological developments and accompanying societal benefits.

We can assume it is unlikely that EU authorities will be conducting a GDPR compliance audit on every company in the world. However, they will probably take action against large incidents (e.g., a data breach like Equifax's in 2017) or if a number of people complain. Recent media reports of Uber's 2016 data breach affecting approximately 57 million users worldwide has led the EU authorities to create a task force to coordinate the national investigations regarding Uber within the EU.

In addition, there are already global frameworks in place to support this kind of effort: The OECD governments have adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, which includes joint enforcement initiatives. The Global Privacy Enforcement Network (GPEN), a network of data protection authorities (DPA) from around the world, was also established to foster cross-border cooperation among privacy authorities.

Even if the EU authorities have difficulties issuing a fine to non-EU organizations, the reputational harm of being in the headlines is starting to take its toll on companies including Uber, Spotify, Plex, Sonos, Unroll.me, Talk Talk and more. In each case, the incidents were widely reported in mainstream media, including *The Wall Street Journal*, *The Washington Post*, *The Guardian*, etc. In some cases (such as Spotify), the CEO had to publicly apologize.

As the EU Commission has now frequently declared, the pursuit of digital markets relies on the development of people's trust. ■

YVES LE ROUX, *CISSP, CISM, is the (ISC)² EMEA Advisory Council co-chair and privacy workgroup lead.*

PAUL LANOIS, *SSCP, CCSK, PCIP, CIPM, CIPT, CIPP, FIP and LLM, is an information security and privacy professional and is vice president and senior legal counsel at an international bank.*

VISIA TARTAGLIONE, *CISSP, ISO27001 LA, is an information security, risk and privacy programs consultant.*

All are members of the (ISC)² EMEA Advisory Council GDPR Task Force.

(ISC)²

SECURITY CONGRESS | APAC 2018

ENRICH
ENABLE
EXCEL

SAVE THE DATE »

9-10 July
Hong Kong

40+ Speakers • 2 Days • 6 Tracks • 35+ Sessions

At (ISC)² Security Congress APAC 2018, you'll get to engage with over 350 security-minded individuals, discover solutions to the latest cybersecurity threats, and gain insight from international industry experts. Maximize your learning experience with our multi-subject sessions, panel discussions, and networking opportunities designed to enrich and enable you to excel as a cybersecurity professional.

Have questions? Talk to us!

Sponsorship - Michaella Park (mpark@isc2.org) | **Registration** - Maggie Yuen (myuen@isc2.org)

In partnership with: image engine

Visit apaccongress.isc2.org

#isc2congressAPAC

DLP

Not an Option Anymore

A practical guide to preventing data leakage

BY MOHAMMAD FAHEEM, CISSP

PROTECTING SENSITIVE DATA continues to be a challenge for businesses of all types, sizes and industry verticals. With growing use of mobile and cloud applications for business activities, along with stringent compliance requirements for sweeping legislation such as GDPR, it is becoming necessary for companies to have visibility and control of their business-critical data. In this situation, data loss prevention, sometimes also referred to as data leak prevention (DLP), is being adopted as a primary tool to monitor and prevent the exfiltration of data outside the organization.

ILLUSTRATION BY JAKOB HINRICHS

Core functionality of DLP largely depends on technology, but is about more than just installing a bunch of tools around your data. Effective DLP is a continuous process of identifying and protecting critical data from leakage, and consists of much more than technology alone.

COMMON CHALLENGES TO SEALING THOSE LEAKS

Some argue that the best way to prevent data loss from malicious insiders is to focus on maintaining the right working environment, culture and corporate policies. However, such incidents would still happen as insider threats are not limited to disgruntled employees. When people handle data, there is always a possibility of loss, perhaps through human error. For example, a CFO's assistant might email confidential financial details to the wrong recipients by mistyping an email address. Or an employee might lose a memory stick with sensitive data on it. Or someone might accidentally install malware by clicking a legitimate-looking link in a spam email.

> Many data-dependent organizations realize that DLP is not a niche IT function, but rather a core capability.

Moreover, compliance requirements imposed by various industry regulators are challenging organizations to prove their ability to protect relative sensitive data from being leaked. The most topical regulation in this context is the EU's General Data Protection Regulation (GDPR), which obliges organizations to identify and report a serious breach of personal data within 72 hours. A DLP solution will enable them to do so.

Many data-dependent organizations realize that DLP is not a niche IT function, but rather a core capability. Protecting data is primarily a business challenge in which technical controls are necessary but not sufficient. Effective risk reduction comes from a balanced, holistic approach, because:

- Data connects employees to the business, so its protection must take into account business objectives, policies, processes and people.
- DLP controls are visible to users and should help them to make informed decisions about data.
- DLP controls require human interaction, so must be designed with humans in mind.

Because of the holistic aspects of good DLP, such programs are usually more complex than many other security solutions. It is prudent to follow industry best practices and a logical step-by-step approach to achieve an efficient and cost-effective DLP solution. The following are guidelines that can help in planning for your DLP program.

Prepare first! Is your organization ready for DLP?

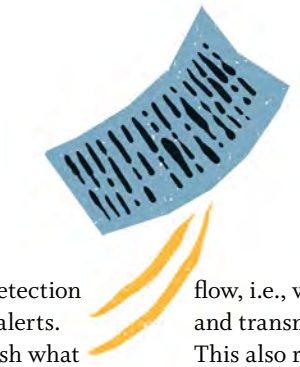
Business engagement. DLP is a business imperative, so you should engage with the key business units and functions as early as possible. The business must understand the importance of protecting data and support the DLP initiative. It can do so by allocating funds and key personnel, identifying the data sets that are critical to their business's functions and appreciating the consequences of critical data being lost or stolen.

Organization and governance. You should map the DLP requirements to your information security strategy and business objectives to determine the success criteria. Identify technical and business stakeholders and clarify their roles and responsibilities. Also prepare a company-wide communication stating the intention of the business to improve data management. DLP controls require human interaction so the employees (end users) must be kept informed and engaged. This can be achieved through continuous communications and training, provided it is visibly driven from senior levels of the business.

Data classification. This is a fundamental element of DLP, as it lays the foundation for an effective data protection strategy. Identify the current data classification levels and corresponding policies and use that information in analyzing and understanding your critical data. In selecting technology, choose the toolsets that can complement each other. For example, a DLP tool can read and append classification tags into documents using a supported data classification solution.

Use business analysis as a tool to identify 'sensitive data'

Data analysis. Should you monitor everything? No. The more data you monitor, the more complex and costly



DLP becomes. It takes time to write complex detection rules, and there is always a danger of needless alerts. Instead, take a smart approach and first establish what data sets are sensitive to your business. This can be done by using pre-defined templates and through discussions with business representatives. Sensitive data may vary for each industry, but the common critical data sets include credit card data, social security numbers, employee data, customer data, trade secrets and pre-patent intellectual property.

> The effectiveness of DLP depends on the detection rules and policies, which should enable monitoring of structured and unstructured data without flagging too many false positives.

Business process analysis. Having identified the sensitive data, you should analyze the relevant business processes to understand how the data—both at rest and in motion—is processed. The resulting use cases are essential if you are to create effective DLP rule definitions. For example, a business process may require a certain business unit to send employee data to third-party screening companies via email. Is there a better way to transmit data securely? Consider a policy to monitor and block if that data is sent by anyone outside that business unit.

Technical planning and maintenance

IT systems analysis. A DLP system needs integration with existing IT infrastructure. Therefore, an analysis of the underpinning IT systems for the selected data sets and business processes enables an understanding of the data flow, i.e., where data sits and how it is accessed, processed and transmitted through different systems and networks. This also reveals any gaps in the infrastructure that may cause problems for DLP implementation.

Architecture and design. Every DLP vendor provides guidelines for performance, sizing and interoperability. These vendor-specific guidelines should be used alongside an IT systems analysis output to document a comprehensive DLP design that fits your requirements. A good design should include the configuration details for core DLP components, i.e., detectors, sensors and the management console. The monitoring coverage should include the protocols and channels such as email, web, applications, end points, network and storage (on premises and cloud), etc., involved in sensitive data handling.

Data capture rules. The effectiveness of DLP depends on the detection rules and policies, which should enable monitoring of structured and unstructured data without flagging too many false positives. The most common search techniques are based on Keyword and Regex (regular expressions). However, more sophisticated DLP solutions provide advanced features to spot violations by applying indexing and hashing algorithms to the data sources. DLP policies should be deployed only after thorough testing and should be periodically reviewed and tuned to maximize effectiveness.

DLP incident management and workflow. Finally, document the operational guidelines and incident workflow for managing DLP alerts. Even the best DLP system cannot be effective without timely triage and response to incidents. The whole purpose of implementing a DLP solution can be wasted if data leakage incidents are not reported to the authorities in time and thoroughly investigated.

A well-planned DLP not only covers organizations on regulatory and compliance fronts, but also boosts their confidence that nothing important will leave unnoticed. If DLP is not part of your IT security strategy, act now, because DLP is no longer optional. ■

MOHAMMAD FAHEEM, *MSc, CISSP, TOGAF, ITIL, CCA, MCITP, MCSE, is a U.K.-based senior security architect with more than 12 years of experience in delivering large-scale IT infrastructure transformation, architecture and security projects. He has exclusive experience in delivering complex DLP programs for customers operating across Europe and Asia with varying regulatory, compliance, language and industry-specific security requirements. He currently is senior manager, cybersecurity for PwC U.K.*

FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

center points

BY PAT CRAVEN

Take Garfield to Work Day on April 26

FOR NEARLY 25 YEARS, on the fourth Thursday in April, millions of parents take their child to work with them as part of Take Our Daughters and Sons to Work® Day (also often called Take Your Child to Work Day or similar title). It is estimated that more than 3.5 million employers took part last year. This international event encourages girls and boys to dream without gender limitations and to think imaginatively about their family, work and community lives. This educational program can help connect what children learn at school with the working world. Plus, it is just plain cool for the kids to see what you do all day and what it is like in the "real world."

This year, we want your help in making the day "Take Garfield to Work Day!"

Last year, we saw a great increase in the number of companies that are now using our Safe and Secure Online and Garfield cybersafety program as part of their commemoration of the day, such as JPMorgan Chase, which I mentioned in the last Center Points article. It is a simple program that we encourage you to discuss with your company leadership and human resources department. Whoever is planning the program for that day will be excited to hear that you have something fun to keep the children busy. There are two programs currently available for this age group.

We have a free, scripted PowerPoint presentation that can be downloaded and is designed for children ages 11-14. This program deals with social media, cyberbullying, passwords, privacy and more.

We also have the Garfield's Cyber Safety Adventures lessons for younger children. Here, companies are picking one of the three available lessons (in English only at the moment) and ordering Educator Kits for their offices. Each kit has everything a group leader needs for 30 children. There are three lessons to choose from: Privacy, Posting and Bullying. You can order the kits online at www.CyberSafetyKits.org. It is a fun way to entertain and educate visiting children. As companies increase the cybersafety awareness of their own workforce, having those same policies and lessons go home with their employees' families can go a long way to making it a safer cyber world.

If you will be placing an order for more than 10 kits for your company, please contact Christina Johnson at cjohnson@isc2.org for assistance. One last tip: Serve Garfield's favorite meal for lunch—lasagna! ■

Pat Craven is the director of the Center for Cyber Safety and Education and can be reached at pcraven@isc2.org.

SCHOLARSHIP REMINDER: DEADLINES APPROACHING

We are currently accepting applications for the 2018 (ISC)² Scholarships, but time is running out. Let anyone you know who is pursuing their cyber or information security education know to apply now at https://www.iamcybersafe.org/scholarships/. Here are the deadlines to remember:

- (ISC)² Women's Information Security Scholarship closed **March 1**
- (ISC)² Undergraduate Information Security Scholarship Application closes **March 15**
- (ISC)² Graduate Information Security Scholarship Application closes **April 17**

lead in

(ISC)² MEMBERS AND EXPERTS FOCUSED ON LEADERSHIP AND PROJECT MANAGEMENT

BRENCIL KAIMBA

Brencil Kaimba is a security consultant in Kenya who has spent the past year mentoring students interested in cybersecurity as a career. She's also mentored girls on cyberbullying. Her devotion to helping others, as well as continuing to demonstrate expertise in both technical and non-technical skills as a lead risk expert at Serianu Limited, helped earn her the first Up-and-Coming Information Security Professional honor at the inaugural (ISC)² EMEA Information Security Leadership Awards (ISLAs).

How did you transition from a degree in mechanical/manufacturing engineering to cybersecurity as a career?

The transition was hard, but my curiosity and need to succeed helped a lot. When I was in college, I didn't know anything about cybersecurity. In fact, I was very passionate about mechanical engineering. After college, I started applying to various companies for a mechanical engineering position, while at the same time visiting schools to encourage students to pursue STEM-related courses. During this time, I met different people and one in particular, Mr. William Makatiani, introduced me to cybersecurity. I was really curious about this line of work and thankfully, he offered me an internship for three months to "test the waters."

Initially, I really struggled with the different IT terms and felt really frustrated whenever I had a technical conversation with the technical teams. There was so much I did not understand, and I had to work twice as hard to reach the level of my other team members. I did a lot of research on cybersecurity trends, standards, best practices, etc., just to keep up.

After all is said and done, I have come to realize that the gap between cybersecurity and other technical fields is not that big. All one needs is the ability to think critically and have a great analytical mind. Cybersecurity is not just IT; it involves strategic thinking, business alignment and process reviews, none of which require extensive IT skills.

Are there many young women working in cybersecurity in Kenya?

No. Few women are involved in cybersecurity compared to men. This is a gap that we (and a few others in the country) are actively trying to close through training initiatives.

Is the number of women in the field growing?

Yes. We are seeing an increase, mainly because there are more initiatives focused on empowering young girls. Programs such as the Serianu-Africa Cyber Immersion program is one of these initiatives, where we intentionally include young girls. More and more hubs and coding camps are forming in Kenya, which has helped to increase the involvement of young girls.

You recently won one of the first EMEA ISLAs for both your work at Serianu Limited and for mentoring Kenyan students through the Cyber Security Training and Awareness for Young People program. What made you take the initiative with both of these organizations?

I was fortunate enough to go to a school where we had different people come and advise us on different aspects of our lives: academic excellence, religion, life, relationships, etc. This helped mold who I am today. Not many people have that. Many students in rural areas are very bright, but lack the guidance, exposure and motivation to help them realize their full potential. Most of these young people are also consumers of new technologies, but they don't understand how to secure themselves while consuming these technologies.

I want to help these young women in the following areas:

- Engage: To know their goals/aspirations/challenges and encourage them to meet these.
- Educate: Educate them on the different cybersecurity concepts, both technical and non-technical, such as how to stay safe online, etc.
- Empower: Let them understand that they can be what they want to be, including cybersecurity professionals. We also want to provide internships and mentoring as they pursue their dreams.

You also mentor young girls on cyberbullying. How big of a problem is cyberbullying in Kenya?

This is a big issue and has sometimes resulted in death. ■

An expanded version of this interview will appear in the April issue of *Insights*, a companion e-newsletter for the (ISC)² membership.

NEW:
KNOWLEDGE SAFARIS
WE'LL HELP YOU FIND THE RIGHT CONTENT SESSIONS AND SUPPLIERS TO MEET

NEW: FAST TRACK PASSES FOR SPEEDY ACCESS AND VISITOR LOUNGE ENTRANCE

NEW: SME SYMPOSIUM
CYBERSECURITY FUNDAMENTALS FOR SME'S

NEW: GEEK STREET
INTERACTIVE AND IMMERSIVE LEARNING FOR ALL OUR TECHIES

NEW: DIGITAL MATCHMAKING
CONTACT VISITORS AND EXHIBITORS TO ASK QUESTIONS, SET UP MEETINGS OR SIMPLY CONNECT

IT IS ALL HERE. YOU JUST NEED TO ATTEND

Over three days the information security industry comes together as more than 19,500+ industry professionals gather to learn, network, experience new products and have fun.

Europe's largest information security event is even better this year, taking over the whole of Olympia with more entrances, more space and more to see than ever before.

Shaping future global industry trends, Infosecurity Europe offers the most cost-effective business and networking opportunities for the world's information security community.

Don't miss out on the number 1 industry event of the year!

05-07 JUNE 2018 OLYMPIA LONDON

REGISTER NOW

www.infosecurityeurope.com

(ISC)² cpe Submitter

@infosecurity