President's Message
Kristina Davis

Thank you to everyone who came out for the Winter Seminar. It was a big success for a chapter – we actually made a little profit for once. I hope everyone enjoyed Mr. Gatto’s presentation. I know I came back more prepared to look further into IT control audits, which was my nugget to take away.

We would like to host another 4-8 CPE seminar in May/June with a speaker or two. Now that the IIA is requiring all CIAs to obtain 2 CPE on ethics, we are looking at providing an Ethics based topic. We have contacted several speakers but they are out of our budget range right now. If you have any suggestions – please reach out to me.

The IIA HQ requested I send out an email earlier to all Chapter Members asking for volunteers for the chapter. The new IIA chapter guidelines require more leadership roles. If you are interested in volunteering and joining up for a leadership, please let either Kristen or myself know. The chapter needs an active membership and volunteer base to keep plugging along.

Hope to see you soon - Kristina

February is the border between winter and spring.
Terri Guillemets
Auditing the Organization's Compliance with the General Data Protection Regulation (GDPR)

March 20, 2018
1:00–2:00 p.m. ET

Many organizations required to comply with the General Data Protection Regulation (GDPR) are finding they must enhance their existing privacy and data protection-related audit programs to address new regulatory requirements. New requirements associated with the GDPR such as broader requirements for privacy notice and consent, the right to be forgotten along with requirements to ensure that third party suppliers are GDPR-compliance create challenges relating to prioritization. Using a case study format, the presenter will share a sample audit plan that addresses the requirements of the GDPR while leveraging data protection impact assessments and privacy by design.

Learning Objectives

In this session, participants will:

- Learn about the key principles associated with the GDPR.
- See a sample audit plan presented to you in a case study format.
- Find out how data protection impact assessments and privacy by design can support the creation of a broad understanding of the organization’s compliance with the GDPR.

Course Duration: 1 hour  
Knowledge Level: Basic  
Prerequisites: None  
Field of Study: Auditing  
Advance Preparation: None  
Delivery Method: Group Internet-based

Speaker

Pamela Hrubey  Managing Director, Crowe Horwath

Dr. Hrubey is a managing director in Crowe’s Risk practice with business experiences in innovation-based organizations spanning from research and development through commercialization. She assists clients around the world in the area of privacy and data protection by assessing the current state of data protection, supporting the construction of robust privacy and data protection programs, and by assisting organizations with the design and implementation of internal assurance programs that support compliance with complex regulatory requirements such as the General Data Protection Regulation. Prior to joining Crowe, Dr. Hrubey’s experiences includes global leadership positions in a top 15 global pharmaceutical company including responsibilities in enterprise risk management, ethics and compliance, global privacy and data protection, clinical data management, medical communications, and human resources development and support.

Go to the IIA website— www.theiia.org  
Click on Training and Events tab  
Select Webinars and register for the webinar - you’ll receive a confirmation email.  
To actually listen to them, you will have to sign into the website with your IIA membership information. You must register and listen to them live to receive the CPE credit.
Truth Is, Fake News Has Always Been a Risk

Misleading or patently false information has long been a risk for organizations. A disparaging comment, even one with little or no foundation in fact, can leave executives scrambling for a response that will contain and, hopefully, reverse any damage. Usually, the truth will prevail.

But as we are seeing more and more, an unceasing barrage of unsubstantiated and outright phony “news stories” powered by social media and biased websites can quickly overwhelm an organization and influence events.

That’s why it was no surprise to me when Google’s parent company, Alphabet, recently elevated objectionable content — specifically, content spreading across the internet and social media — as a key risk. Alphabet’s concern, of course, regards the integrity of its own brands, but the risk applies to any organization and, indeed, any individual.

“Our brands may be negatively impacted by a number of factors, including, among others, reputational issues, third-party content shared on our platforms, data privacy issues and developments, and product or technical performance failures,” Alphabet stated in its annual report, or 10-K, to the U.S. Securities and Exchange Commission. “If we fail to appropriately respond to the sharing of objectionable content on our services or objectionable practices by advertisers, or to otherwise adequately address user concerns, our users may lose confidence in our brands.”

Did this risk just occur to executives at Alphabet? I highly doubt that. What’s different, I believe, is the company’s risk appetite.

The recent backlash against questionable content bombarding consumers of Alphabet’s YouTube and Google, as well as Facebook and Twitter, are clearly driving the change.

Frankly, the company’s description of risk might be considered by some as pretty mild. It doesn’t warn of the societal dangers of objectionable content, but of the risk of losing advertisers and users of its services if it fails to respond appropriately. It also doesn’t address an erosion of public confidence in legitimate media posed by questionable reports masquerading as news; rather, it focuses on “third parties” that are exploiting Alphabet’s brands to spread the false information.

Striking a balance between a free flow of information, even if it’s titillating or scandalous, and acting responsibly as a reliable and credible conduit for such “news” is nothing new. Organizations, including mainstream media, have played that game for centuries.

The lesson for internal auditors is that we must be attuned to our organization’s risk appetite and offer warnings when the risks change. This may be what is driving the change in tone from Alphabet.

Speaking at The IIA’s 2016 General Audit Management conference, Google’s chief audit executive said the organization’s internal audit function is practically built on that premise: “Our mission is to provide an objective view of all the risk they need to consider in making their decisions. Our responsibility is to help management have full information to make good risk-based decisions.”

Ultimately, it is up to management and the board to set the risk appetite, but it falls on internal audit to make sure the risk portfolio is accurately reported all the way to the top. In Alphabet’s case, I’m confident management and the board are fully aware of the undercurrents of information dissemination, and that they will continue to adjust their risk appetite to fit those changing dynamics.
In pondering the very real risk of fake news, I am reminded of the story of a famous radio broadcast in 1938. Orson Welles, an American actor, writer, director, and producer, “interrupted” CBS radio programming with breaking “news” that Martians had invaded Earth. He was actually reading from author H.G. Wells’ science fiction novel, “The War of the Worlds.” But his delivery was so compelling and so realistic that, for some listeners, it was also very believable and set off a panic. The iconic broadcast and the reaction of those who thought it was real have been part of lore for decades. Yet, a 2013 article cast doubt on the fact that the broadcast caused panic. So, now even the news about the fake news may be fake. We are living in interesting times.

As always, I look forward to your comments

---

**IIA Releases Updated GTAG on IT Governance**

Recognizing the integral role and competitive advantage that IT can provide organizations, The IIA has released an updated Global Technology Audit Guide (GTAG), Auditing IT Governance to help internal auditors add value in this space. The update provides a high-level overview of IT governance and highlights important factors in developing a successful IT governance approach including:

- Assessing the degree to which governance activities and standards are consistent with the internal audit activity’s understanding of the organization’s risk appetite.
- Conducting consulting engagements as allowed by the audit charter and approved by the board.
- Fostering an ongoing dialogue with the IT governance activity to ensure that substantial organizational and risk changes are being addressed in a timely manner.

The guide also includes tools and resources to help in the process, such as guidelines for conducting an IT governance engagement, an internal controls questionnaire, and an IT governance risk and control matrix example. IIA members are invited to download guidance as a benefit of membership. Nonmembers may purchase guidance by visiting The IIA Bookstore.

**New Practical Enterprise Risk Management Book Released**

The IIA Bookstore’s newest release, Practical Enterprise Risk Management: Getting to the Truth, takes a no-nonsense approach to helping enterprise risk management (ERM) champions effectively employ ERM approaches to help their organizations reach their goals. By offering a “how-to” application with step-by-step descriptions of two practical ERM approaches, author Larry Baker empowers readers to tap into what one chief executive officer Baker worked with described as ERM’s value: “It gets to the truth.”

The book is an easy-to-read resource that communicates the vast landscape ERM covers in easy-to-understand, actionable laymen’s terms. It illustrates the importance of ERM fundamentals by using real-world examples drawn from Baker’s more than 20 years of ERM experience. Complete with supporting forms, tools, and templates that he used with clients and past employers, the book allows readers to develop an effective, customized, and sustainable ERM approach for their organizations.

Written by an ERM practitioner, Practical Enterprise Risk Management: Getting to the Truth offers something for every level of experience, whether you are seasoned in the field or it is the first day of your first ERM assignment. Readers will gain the greatest lessons learned from Baker’s more than 40,000 hours of ERM work. Visit the IIA Bookstore to learn more.
IIA Announces Key Updates to CIA Certification Exam

The Institute of Internal Auditors (IIA) announces important updates to the Certified Internal Auditor (CIA) Examination. This three-part exam is designed to test candidates’ knowledge, skills, and abilities related to current global internal audit practices.

To ensure the exam’s content remains current and valid, the CIA underwent a job analysis study, with The IIA reaching out to candidates, certification holders, academics, experienced internal audit professionals, and other stakeholders around the world to determine the knowledge, skills, and abilities most relevant to today’s internal audit professionals.

Results of the study confirmed the need to revise the exam syllabi to reflect the evolution of the internal audit profession worldwide.

Launched in 1974, the CIA exam is administered in more than 800 testing facilities in more than 150 countries and territories around the world.

The Rising Tide of Cyber Risks

Corporate leaders are rethinking business plans in response to information security threats.

Tim McCollum Internal Auditor January 25, 2018

Large-scale cyberattacks rank third in likelihood among global risks identified by the World Economic Forum’s Global Risk Report 2018. Released this month ahead of the forum’s annual gathering of world and business leaders in Davos, Switzerland, the survey report predicts a heightened global risk environment, with the tentacles of cyber threats factoring into business and geopolitical risks. Think cyberwarfare and attacks on major companies, banks, and markets.

"Geopolitical friction is contributing to a surge in the scale and sophistication of cyberattacks," says John Drzik, president of Global Risk and Digital with insurer Marsh, in a press release accompanying the report. That risk continues to grow for businesses, as well, even as they become more aware of cyber threats, Drzik points out. "While cyber risk management is improving, business and government need to invest far more in resilience efforts" to avoid protection gaps.

Dire warnings about cyber threats are pushing boards to reconsider their business plans. In EY’s latest Global Information Security Survey, 56 percent of C-suite respondents say the increased impact of cyber threats and vulnerabilities has led their organization to change or plan to change business strategies. Only 4 percent say they have fully considered the security issues arising from their current strategy.

It’s not the large-scale attacks envisioned by the World Economic Forum report that worry the nearly 1,200 respondents to the EY survey. It’s the less sophisticated attackers that have targeted their organizations. "The most
successful recent cyberattacks employed common methods that leveraged known vulnerabilities of organizations,” says Paul van Kessel, cybersecurity leader for EY’s Global Advisory.

Couple that with new technologies and increased connectivity, and organizations are facing more vulnerabilities than before, he notes. As they look to transform their businesses, organizations need to assess their digital environment “from every angle to protect their businesses today, tomorrow, and far into the future,” he says.

**A Question of Money**

Executives clearly see a need for more resources to face cyber threats. Although 59 percent of respondents say their cybersecurity budgets increased in 2017, 87 percent say they need to allocate as much as 50 percent more. Twelve percent expect more than a 25 percent increase this year.

For many organizations, it might take a major breach for them to make significant cybersecurity investments, respondents report. Three-fourths of respondents say an incident that caused damage would result in a higher cybersecurity outlay. Conversely, nearly two-thirds say a less damaging attack would not lead to an increase.

**Three Levels of Attack**

Budgets aside, respondents acknowledge the vulnerabilities and threats are rising. Chief among the vulnerabilities are employees who aren’t following good cybersecurity practices. Malware and phishing far outpace other threats.

In the face of increased threats, resilience may be the best way for organizations to fight back. “To get there, the organization needs to understand the relationship between cyber resilience and the objectives of the business, as well as the nature of the risks it is facing and the status of the current safeguards,” the EY report says. “It must also assess how much risk it is prepared to take and define an acceptable loss.”

To become more resilient, the EY report notes that organizations need to take steps to address three levels of attack: common, advanced, and emerging.

**Common.** Although the vast majority of attacks target known weaknesses, three-fourths of respondents say their organization’s ability to identify vulnerabilities is immature or moderately mature. Twelve percent lack a breach detection program, and 35 percent say their data protection policies are ad hoc or don’t exist.

To defend against common threats, EY proposes five components:

- Talent-centric, with everyone in the organization responsible for cybersecurity.
- Strategic and innovative, with cybersecurity embedded into decision-making.
- Risk-focused, with “well-governed risk alignment.”
- Intelligent and agile, to detect and respond to threats timely.
- Resilient and scalable, to minimize disruptions and grow with the business.

**Advanced.** These sophisticated attacks target unknown or complex vulnerabilities, and are carried out by organized crime groups, cyber terrorists, and nation states. To respond to such attacks, the EY report recommends organizations
centralize cybersecurity activities within a security operations center (SOC). This center should focus on protecting the organization's most valuable assets, defining normal operating conditions as a basis for identifying unusual activity, gathering threat intelligence, and carrying out "active defense" missions to identify hidden intruders.

**Emerging.** These unanticipated attacks are made possible by advancing technologies. Responding to them requires agility to imagine the attacks that could be possible and act quickly when they happen, the report notes.

**In Case of Emergency**

Beyond these measures, the EY report says organizations need a cyber breach response plan that automatically springs into action when an incident occurs. The cybersecurity function plays a part, but the plan also involves business continuity planning, compliance, insurance, legal, and public relations. This is an area where many respondents fall short. Nearly 70 percent have a formal incident response capacity, but problems arise when drilling down to specifics.

Communication is a glaring problem, with 43 percent saying their organization doesn't have a communication strategy to respond to attacks. Just 56 percent say they would notify the media within a month of an incident that compromised data. That could prove costly, with the European Union's Global Data Protection Regulation set to take effect in May. Organizations that fail to respond timely to data breaches could face tangible penalties beyond the damage caused by attacks.